Audio Networks
An Overview
2001

BIAMP

from BIAMP Technical Training Manual

音響特機株式会社
http://www.otk.co.jp info@otk.co.jp
東京都千代田区麹町 2-5 TEL 03-3237-1201
大阪市北区東天満 2-10-24 TEL 06-6357-0160
福岡市南区野間 1-1-19-403 TEL 092-554-6066

音声ネットワークがふさわしい方法だと判断するとき 1
はじめに 1
施設の概観 1
距離とチャンネル数 2
他のネットワーク必要条件と既存のインフラ 2
求められる柔軟性 2
制御と監視 2
バックアップ機能と信頼性の必要条件 3
将来の拡張 3
材料と人件費 3
スタジアムの例 4
コンベンション・センターの例 5

Ethernetの歴史と背景 6
はじめに 6
最初の Ethernet.....6
CSMA/CD.....6
Ethernet パケットの構成 7
Ethernet の規格 7
10BASE-T.....8
100BASE Ethernet.....8
ファスト Ethernet のバリエーション 9
ギガビット Ethernet.....9
ギガビット Ethernet のバリエーション 9
将来 9

プロジェクトにふさわしいケーブルを選択する 10
はじめに 10
ケーブルプラント 10
CAT5 10
距離の限界 10
コネクター 10
ツイストと終端 11
ストレートケーブル VS クロスケーブル 12
クロスケーブルとアップリンクポート 12
光ファイバーケーブル 12
コネクター 13
配線とネットワークの特性 13
CAT5 とケーブルタイ 14
引く力と曲げるときの半径 14

プロジェクトにふさわしいハードウェアを選択する 15
はじめに 15
データ端末装置 15
データ通信装置とEthernet ハードウェア 15
ネットワークインターフェースカード 15
リピーターハブ 15
スイッチングハブ 16
リピーターハブ対スイッチングハブ 19
ブリッジとルーター 19
リンクを確立する 20
10Mbps ネットワーク 20
100Mbps デバイス 20
オートネゴシエーションするデバイス 20
オートネゴシエーションの例 21
メディアコンバータ 21
ネットワークアドレスをアサインする 22
IP アドレス 22
サブネットとサブネットマスク 23
クラスレスアドレス 24
IP アドレスと音声ネットワーク 24
ネットワークの設計と構築 24
PCに IP アドレスを割り当てる 25
スイッチングハブを配置する 25
接続テスト 25

ネットワークで音声をルーティングする 26
はじめに 26
ファイルを転送してから再生する 26
メリット 26
デメリット 26
用途 26
ネットワーク越しの再生…「引っ張る」モデル 26
メリット 27
デメリット 27
用途 27
ネットワーク越しの再生…「押し込む」モデル 27
メリット 27
デメリット 27
同期ストリーミング 27
メリット 28
デメリット 28
アイソクロナス・ストリーミング 28
アイソクロナス転送の送信機と受信機 28
メリット 29
デメリット 29
CobraNet 30
CobraNet 用語 30
CobraNet インタフェース 31
アイソクロナス・サイクル 31
コンダクタ 32
コンダクタの調停 32
CobraNetプロトコル 33
ビートパケット 33
リザベーションパケット 33
音声データパケット 34

ネットワークの管理と制御 35
はじめに 35
ネットワーク管理とは? 35
Telnet、HTTP、FTP.....35
TELNET.....35
HTTP.....35
TFTP.....36
SNMP を使った管理 36
エージェントマネージャーと MIB.....37
エージェント 37
MIB.....37

マネージャー 37
SNMP メッセージ 37
管理ソフトウェア 38
ポーリングとネットワークトポロジー 39
部分表示 39
イベントログと特性 39

特殊なニーズに合わせて設計されたネットワーク 40
高可用性 40
高可用性デザイン 40
質が高いコンポーネント 40
コールドスペア 40
ホットスワップ 40
故障時の切り替え 40
障害に対する強さ 40
環境の要因 40
監視 40
生命の安全 41
ネットワークの可用性 41
リンクアグリゲーション(トランキング) 41
スパニングツリープロトコル 42
メッシュ 43
音声インタフェースの有効性 43
インタフェースデバイスを対にする 43
バディリンク 43
デュアリンク 43
ネットワークを混在させる 43
ブロックしないスイッチングネットワークデザイン 44
バーチャル・ローカルエリア・ネットワーク 44
QoS 44
大きな設備 45
コアスイッチを使う 45
音声のVLAN 45
レイヤー3ルーティング 46
距離とスイッチホップ 46
フォワーディングディレイ 46
遅延の変動 46

音声ネットワークのトラブルシューティング 47
はじめに 47
当たり前のことを確認する 47
リンクを調べる 47
管理機能を持つスイッチングハブの設定 47
LEDがエラーを示している 47
音声をチェックしよう 47
信号の有無 47
音質 48

Chapter 1　音声ネットワークがふさわしい方法だと判断するとき

はじめに

ネットワークはあらゆる専門システムに大きな影響を与えてきた。商業ビルの多くにはネットワークインフラが設備されている。このネットワークで一般的なコンピュータデータと共に、照明、セキュリティ、販売情報などさまざまなデータを伝送できる。世界は本当にネットワークワールドになったのだ。音声はといえば、つい最近まで建物に張り巡らされたこのデータインフラには入っていなかった。いつも独立した一般的なアナログ配線のシステムだった。

完全に独立した配線構造の設置が必要だということは、材料や労働と時間のコストを大幅に増大させる可能性があるということだ。プロジェクトによっては重要な要素だろう。

ネットワークで音声を分配することには、もちろんコストという要因以外に多くの利点がある。柔軟性は大いに向上する。適切に設計すればどんな音声入力をどんな音声出力にでも、配線し直したりパッチベイを使うことなくルーティングできる。この能力によって機器や配線を変えることなくシステムの構成を変更したり、将来の改修にも対応できる。

音声ネットワークならバックアップを持たせることも故障に強いシステムにすることもできる。ネットワーク上の機器やケーブルが損傷したとき自動的に切り替わるよう設計することも可能だ。従来のアナログシステムではケーブルが切れればまず問題の箇所を発見し、それから交換するか修理するか、パッチして迂回しなければならない。ネットワークなら中央のパソコンから管理機能ですべてのネットワーク製品を監視し、障害の発生時に警告を出させることもできる。

ネットワークシステムは最終的にケーブルやインフラを大幅に縮小させるし、音声を伝送するケーブルに制御と監視のデータを運ばせることもできるのだ。

ある現場に音声ネットワークが適切かどうか定義するとき、従来の配線が何を意味するか広く深く考えなければならない。ネットワークはかつて実現できなかった新しい機能を提供する。その新しい可能性をどこに使えばシステムが良くなるのか考えるには、新しい機能を学ばなければならないしシステム設計のスキルや知識を駆使しなければならない。好きなチャンネルをどんな出力へも送れるだけでも新しい方法を考える価値はある。ネットワークの利点を学ばなければ取り残されるだろう。反面、点同士をアナログで接続することが最善なら新技術に惚れ込む必要はない。この講座が終わると皆さんは前進し、そしてこの業界をネットワーク世界に導いていくための知識を身につけているはずだ。

ネットワークで音声を分配する設計には多くの利点があるが、常に正しい解決であるとは限らない。この章では音声システムのニーズを調べ、音声ネットワークがあるプロジェクトにとって利益になるかどうか定義する方法を紹介する。

施設の概観

あるプロジェクトにネットワークがふさわしいかどうか判断するとき、判定すべき基準がいくつかある。

- プロジェクトの概要
- 機器の設置場所
- ルーティングの必要性
- 距離
- チャンネル数
- 他のネットワークインフラと既存のインフラ
- 求められる柔軟性
- 制御と監視の必要条件
- バックアップ機能と信頼性
- 将来の拡張要求
- 材料費
- 人件費

ネットワークが適しているかどうか定義する最初のステップは大局を見ることだ。音声入力や音声出力、機器は何カ所にあるだろうか？システムはどこで制御するのか？システムの大きさは？場所同士の距離は？顧客は「技術志向」か？

機器をすべて同じラックに入れる場合ネットワークが良いとはいえないだろう。ネットワークの利点の１つは音声とデータを遠く離れた場所に送る能力だ。まず機器、入力、出力の場所と制御する場所をすべて定義しよう。一般的には場所の数が増えると音声ネットワークが便利になる。

次に必要とされる音声ルーティングを定義する。すべての音声をすべての場所にマトリクスで送るのか、それとも点から点へ送ればいいのか？特定のイベントによってルーティングを変えることがあるか？その例が時間単位での変更を求められるコンベンション・センターだ。ある日は会議室が特定の宴会場と関連づけられ、次の日は隣りの大ホールから音声をもらうよう設定されるといった具合だ。必要性は時間が経てば変わるだろうか？議事堂や議場は選挙の後、特にメンバーの過半数や議長職が代わると変更されることが多い。システム設計が完了した後で実際のルーティングを変更することはあるだろうか？テーマパークがこの例だ。インフラはショー自体より先に設計が完了していなければならない。プロジェクトの終了間際までニーズが定義されないことも多い。終盤でもルーティングを変更できる柔軟性を持つ

ネットワークは魅力的な解決法になるだろう。

調整室とアンプ室だけを接続するだけでルーティングを変更しないならアナログの方が適しているかもしれない。

距離とチャンネル数

ネットワークがふさわしいかどうか決めるとき、場所同士の距離も重要だ。一般的には距離が長くなればネットワークが適しているが、距離が短くてもルーティングの必要性や他の要因によってネットワークの方が良いかもしれない。CobraNet なら CAT5 ケーブル 1 本で 100m まで接続でき、各方向に 64 チャネル (合計 128 チャネル) を伝送することができる。マルチモード光ファイバーケーブルなら 2km まで伝送できる。ギガビットのスイッチング Ethernet なら 1 千以上のチャネルを伝送することも可能だ。

設計するとき機器と設置場所ごとに必要な入力と出力の数を定義しておくべきだろう。設置場所の間で伝送が必要なチャネル数を知っておくことも同じように有用だ。

他のネットワーク必要条件と既存のインフラ

その施設で他のデータが伝送されていないか定義することも有用だ。新設なら他の分野でデータ伝送が必要ではないか調べてみよう。照明やセキュリティ用に Ethernet ネットワークが設計されていて余裕があるかもしれない。そのバンドワイズを使えれば音声システムのコストを大幅に削減できる。IT チームが設計した施設全体のネットワークに音声をのせてもらえるかもしれない。こうなれば大幅に減らした予算を音声システムの他の部分に回せる。別の目的でデータネットワークを設計している部署はないだろうか？ その人たちと協力すればインフラコストを分担できる。

心にとどめていただきたいのは、ネットワークがスイッチングであれば Ethernet を利用した音声関連のデータを他の目的で分配されるデータと同じケーブルで伝送できる、つまりネットワークを共用できるということだ。

既存の施設を改修する場合、既設のネットワークインフラを探してみよう。能力に余裕があるか？ 都合の良い場所まで届いているか？ またアナログインフラも同じように調べよう。場合によっては利用できるコンジットが見つかるかもしれない。ケーブルトレーシステムはあるだろうか？

求められる柔軟性

従来の配線は「点から点へ」の変形だ。つまり信号が常にある 1 点から別の 1 点に送られることで接続が固定されている。配線についてはアナログでもデジタルでもこの通りだ。AES/EBU はデジタル信号だがある点と別の点を結んでいるだけだ。接続が固定されればシステムは限定されたものになり 1 つの方法でしか機能しない。柔軟性はないし構成を変更することもできない。

システムにいくらかでも柔軟性を持たせるときは「パッチベイ」を入れるのがふつうだろう。これで音声のルーティングは変えられるようになったが、まだかなり限定されている。音声が向かうそれぞれの拠点にはパッチベイにルーティングを変更するためだけのケーブルを設置しなければならない。パッチベイそのもので対応できるシグナルパスは限られていてあまり柔軟性はない。またパッチベイを操作するには専門知識が必要だ。さらにハム、大音量のポップ、ノイズなどの問題を発生する原因になる可能性もある。

ネットワークでは音声チャネルをすべて (設計にもよるが) ネットワーク上のどこにでも送れる。もう信号を帰すためにケーブルを対にする必要はないし、柔軟性は大きく向上する。また現場で簡単に設定できる。チャンネルのルーティングをプリセットに保存しておけるので、特定のイベントに合わせて配線を完全に変えられる。将来変更が必要になったときも、そのニーズに合わせることが可能だ。ネットワークを設計するということは十分な能力とノードを確保できることであり、実際に将来を考えるわけではないが現場に必要な以上のものを入れておける。テーマパークは基本設計の完了期限を過ぎても微調整が続く現場だが、この能力がいかに有用かを証明できる場所でもある。これは大いなる柔軟性だ。こんな柔軟性と設定変更能力は皆さんのプロジェクトに必要ないだろうか。

今までこんな機会はなかったが、これからはこうした新しい能力の持つ潜在的なメリットについて考えなくてはならない。従来の点と点を配線するシステムも機能はするだろう。しかしこうした新しい能力が皆さんのプロジェクトに有益であることを証明できるかもしれない。一方でこんな能力はどれも不要かもしれない。この講座で皆さんがご自身でそれを決めるための知識を学ばれることだろう。

制御と監視

制御と監視には 2 つの種類がある。1 つはネットワーク自身の制御と監視だ。ここにはケーブル、スイッチングハブのようなネットワーク製品、ネットワーク上でデータを生成したり使ったりする実際の製品が含まれる。たとえばネットワークに接続されているパワーアンプにはネットワークインタフェースが内蔵されているだろう。そのカードが正常に動作しているかを確認するために監視したいと考えることもあるだろう。それがネットワーク上の離れた場所からできるのだ。

市場にはさまざまな機能を持った製品が出回っている。ネットワーク上のどこかで障害が発生したとき警告を発してくれ、トラブルを簡単に診断できる機能だ。こういう監視は信頼性とネットワーク診断能力を向上する。音声ネットワークがあるプロジェクトにふさわしいかどうか決めるとき、こん

な能力についても熟慮しなければならない。

もう１つは、先ほどのアンプの例なら離れた場所からクリップ LED を監視したり、レベルを調整するようなことだ。CobraNet ならさまざまな制御と監視データを伝送できる。ネットワークがデータを伝送し、機器メーカーが制御データを提供する。この例が QSControl、MediaMatrix、IQ、RaneWare、NexSys などだ。重要なことは CobraNet とこうした制御・監視ソフトウェアを併用するときは、たいてい音声データと制御・監視データを一緒に CAT5 や光ファイバーケーブル１本で伝送しているという事実だ。これで全体が簡素化され、別のインフラが不要になって配線コストを削減できる。たった１本のケーブルを配線するだけで設備工事やトラブルシューティングの手間が大いに減少する。この種の制御システムや監視システムを使う場合は重要な要因になり得るだろう。こうした技術が不要ならそのプロジェクトにネットワークを導入するメリットはないかもしれない。

バックアップ機能と信頼性の必要条件

Ethernet は世界中のさまざまな分野で多くの任務で不可欠な用途に使われている。バックアップや故障への対応には長い間のノウハウがあるし、プロジェクトに合わせて解決法が選べる。ニーズに対する取り組みが進んでいるということは、確立した技術を利用するメリットの１つだ。開発されたばかりの新しい技術ではまず問題を発見しなければならないし、解決はその後になる。さらにテストと最終調整をしなければならない。時間がかかるし、最初のうちはたいてい時間を浪費して落胆するような経験の積み重ねになる。

一方 Ethernet なら前述のように「管理機能を持つ」スイッチングハブのように離れた場所から監視できる製品もある。ネットワーク管理ソフトを使ってネットワークの動きをすべて監視することができる。これで信頼性は大幅に改善する。

冗長性という利点によって、完全なバックアップシステムはもちろん、さまざまなレベルのバックアップシステムを設計可能だ。完全なバックアップとはケーブルと機器をすべて２つずつ設置して平行して運用するシステムだ。機器やケーブルがネットワーク上で損傷すると自動的に検出され、その部分がバックアップに切り替わる。人間が介在することなく切り替えられるしまったくシームレスだ。ケーブルが切れてもシステム上では音声が出力され続けるのだ。

バックアップ機能はそれほど必要ない、あるいは他のやり方で故障に強いシステムを作るなら、コストはより下げられるだろう。従来の接続で心線が切れた、コネクターが損傷した、製品が故障したといった場合、人間が対策を考えることになり手作業で修繕するだ。パッチベイを使って適切に設計されたシステムなら簡単に順応できるだろう。あるいは修繕には時間がかかってもかまわない現場もある。デジタル音声がもたらすもう１つのメリットは、特に光ファイバーケーブルを使うと RFI(無線周波数干渉) の被害を受けにくくなることだ。音声ネットワークはすべてデジタルなので、このおまけともいえるメリットを享受できる。

将来の拡張

よく考えられたシステムなら将来の拡張に対応できる。ネットワークシステムにはインフラ拡張に備えるというメリットもある。既存のネットワークにノードや製品を追加するのは簡単だ。アナログシステムで新しい場所に機器を設置する場合、ケーブルやコンジットなどを追加しなければならないことが多い。もちろん将来の拡張がミキシングコンソールを大きくするだけ、あるいはラックに新しい機器を追加する程度ですむなら、ネットワークにするメリットはないかもしれない。将来の拡張が新しい場所に機器を設置することや分配チャンネルを増やすこと、ルーティング変更の能力を必要とするならネットワークが本当のメリットを提供することになる。

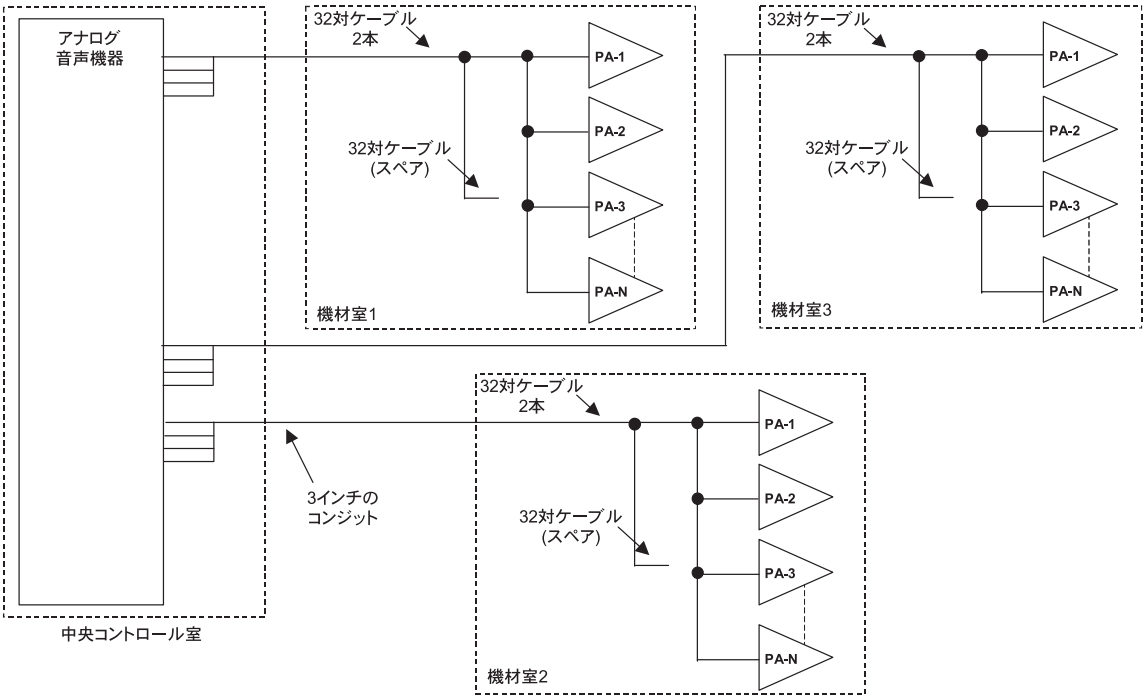
材料と人件費

ネットワーク音声システムに必要な材料は、従来のアナログやデジタルシステムに使うものとは違う。ネットワーク独自のものとして Ethernet スイッチングハブのコスト、さらに管理機能を持たせる場合は管理ソフトウェアのコストが加わる。しかしネットワーク化すれば他のインフラコストが大幅に減少する。たとえば大きな施設ではコンジットの中をマルチケーブルがたくさん通る。その先にはマルチコネクターを取り付ける。コンジットが長くなるほど材料費が高くなるだろう。ケーブルにコネクターを取り付けるには時間がかかるし、当然ながら人件費も上がる。コンジットの設置も労働力がかなり必要なので人件費が上昇する。さらにこうしたシステムで異常が発生すれば、解決するためにまた人件費がかかる。もちろんレストランやバーのような小さい施設ではさほどケーブルは多くないだろうし、材料費や人件費はそれほど高くならないだろう。

ギガビットのスイッチング Ethernet ならを１対の光ファイバーケーブルで１千以上のチャネルを伝送することができる。またコンジットを通す必要がないので、材料費と人件費の両方をかなり圧縮可能だ。CAT5 ケーブルを使った標準的な CobraNet でさえ合計 128 チャネルを伝送できる。コネクターはクリンプタイプか光ファイバー用のもので、はんだ付けはいらないし設置も簡単だ。一般的な音声コネクターを処理するときに必要とされる専門的な技能はいらない。システムの必要条件にしたがって音声ネットワークを使えば、かなり大幅なコスト削減もあり得るのだ。コストと設計のサンプルをこれから比較してみよう。

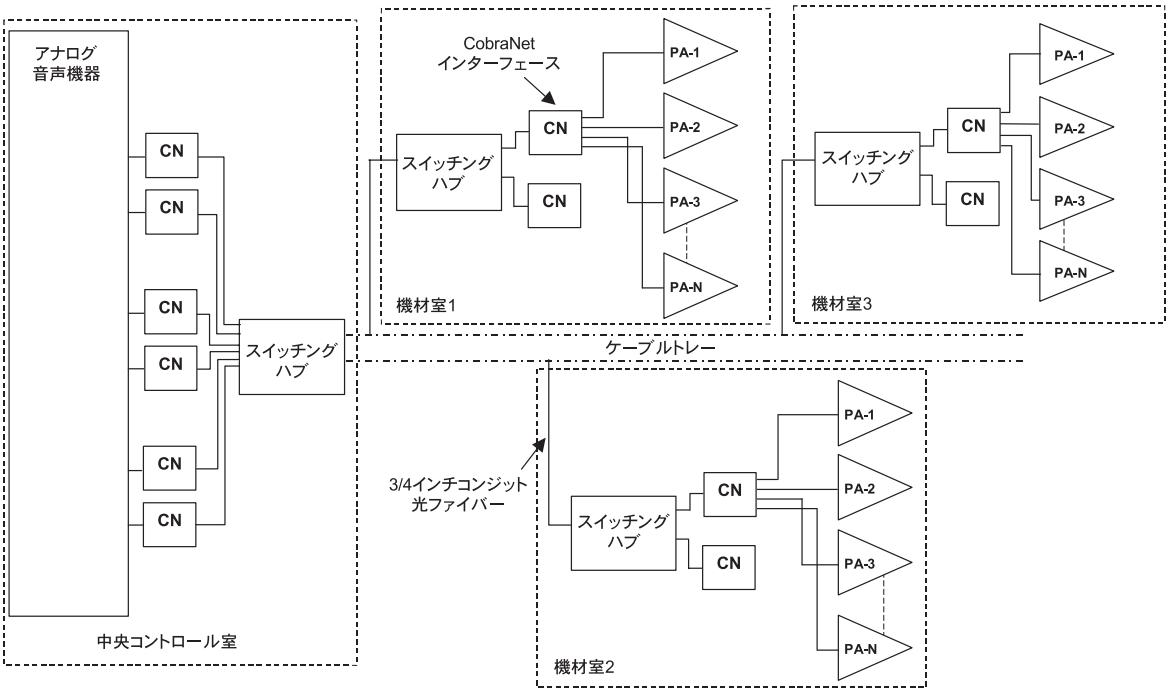
スタジアムの例

アナログの場合は 4600 フィートのケーブルを使いコンジットはほとんど 3 インチだ。ケーブルとコンジットの費用は 44,700 ドル、人件費が 1,500 ドルと見積もられたので、アナログシステムのインフラにかかる費用の合計は 46,200 ドルということになる。



従来のアナログシステム

ネットワークで設計するとより複雑に見えるかもしれないが、インフラという見地からすれば実はかなり単純でコストはかからない。ネットワークなら少ないケーブルでより多くのチャンネルを伝送できるし、既存のケーブルトレーに光ファイバーを通すことにしたため、インフラコストは 3,000 ドルを下回った。

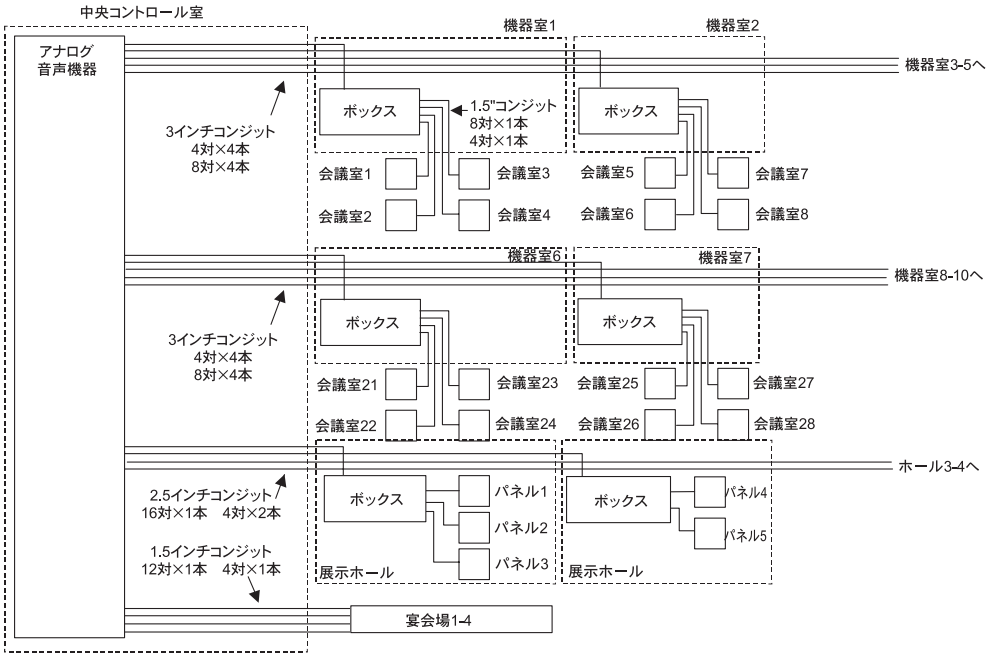


CobraNetシステム

コンベンション・センターの例

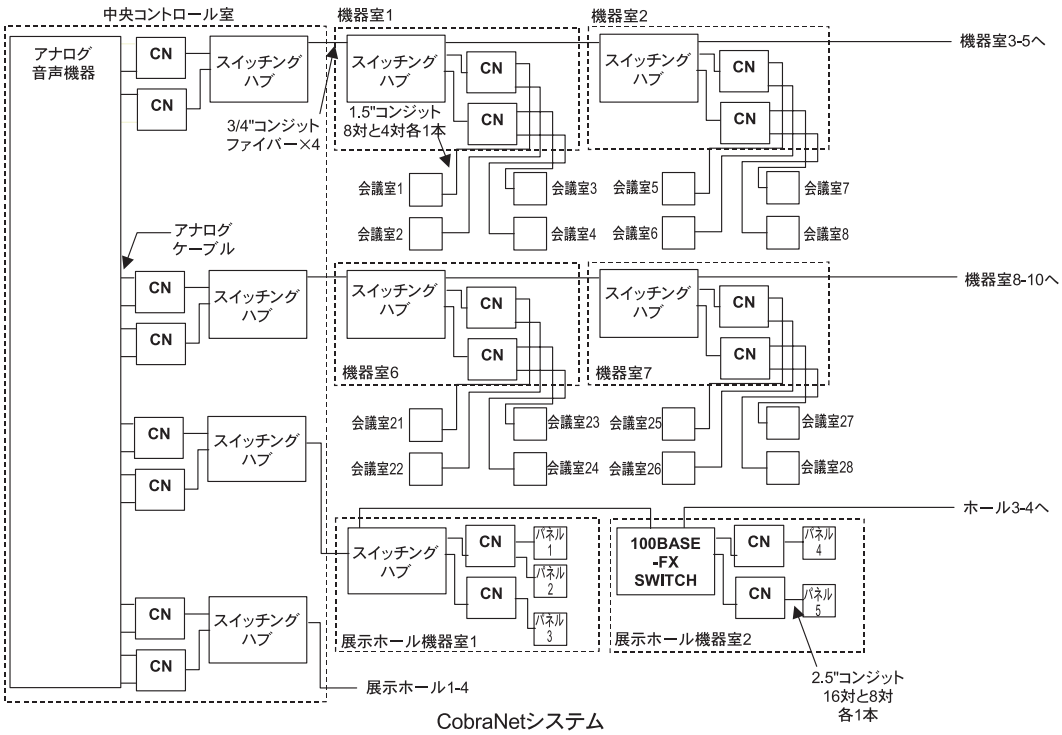
8 対と 4 対のマルチケーブルを 1.5 インチのコンジットに通し、100 フィート引き回して 4 つの会議室それぞれと離れた場所にある機材室を接続している。機材室から各会議室まで帰るケーブルは 3 インチのコンジットを通っている。その中には 8 対と 4 対のマルチケーブルが 4 本ずつ入っている。この例では会議室のコストだけ見てみよう。

コンジットとケーブルにかかるコストはほとんど 160,000 ドルに近く、設置にかかる人件費は 8,000 ドルをやや超える。インフラコストは合計で 163,000 ドルだった。



従来のアナログシステム

ネットワークではやはり機器が増えているがインフラはより単純だ。CobraNet を使って 3/4 インチのコンジット 1000 フィートで北側と南側の機材室を結ぶ。合計で 3/4 インチのコンジットを 2000 フィートと 1.5 インチのコンジットを 4000 フィート使って機材室の I/O パネルを接続した。コンジットとケーブルにかかったコストは 30,000 ドルだ。人件費を足すとインフラコストは合計 36,700 ドルになる。



CobraNetシステム

Chapter 2　Ethernet の歴史と背景

はじめに

1972 年にゼロックス・パロ・アルト研究センター (PARC) のロバート・メトカーフたちははじめて相互接続用の実験的な Ethernet システム、ゼロックスアルトを開発した。最初はアルトアロハネットワークと呼ばれていたが、1973 年にメトカーフは名前を「Ethernet」に変えた。

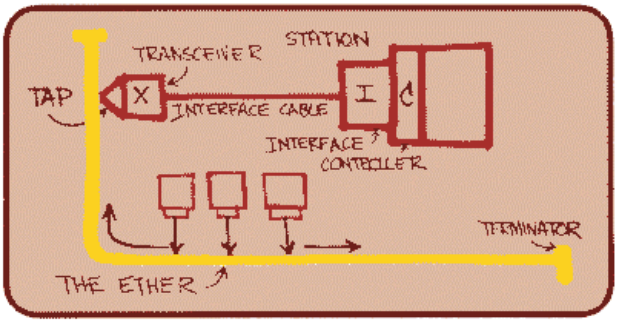


図 2-1　最初の Ethernet

最初の Ethernet

最初の Ethernet はネットワークに接続した全ステーションで利用可能なバンドワイズを分かち合い、メディアを共用するものとして機能した。1 つのステーションから送信されたものをすべてのステーションで受信するシステムだったが、一度に送信できるステーションは 1 台だけだった。複数の機器から同時に送信すると衝突、つまりコリジョンが発生してしまうためだ。ほとんどのメッセージはコリジョンにゆがめられていた。当初コリジョンはメディアを共用する Ethernet ネットワークにおける活動の事実であり、ほとんどの状況では問題ないものと考えられていた。しかし実際にはネットワークへのアクセスを管理し、コリジョンを妨いで回復するためのメカニズムが必要になった。

CSMA/CD

Ethernet で採用されたメディアアクセスの方法が CSMA/CD(Carrier Sense, Multiple Access with Collision Detection) だ。Carrier Sense とは、データを送信しようとするステーションが、他のステーションからデータが送信されていないか「聞く」ことを意味している。他のステーションが通信している場合はキャリア信号が聞こえるまで待機するのだ。Multiple Access とは、1 本のケーブルでたくさんのステーションに伝送の機会を与えることだ。あるステーションが送信し終わるとすぐに他のステーションがアクセスできるようになる。Collision Detection とは、複数のステーションからの同時送信を検出するプロセスだ。

ネットワーク直径とは最も離れた 2 つのステーション間の距離を指すが、これが 2000m を超えるほど大きくなると両端にあるステーションでは受信したデータが破損していることもあった。両方のステーションで同時に信号を送り始めると小さいデータパケット (パケットはすべてもう伝送ケーブル上を移動中だ) がケーブル上で衝突し、破損した状態で受信するステーションに送られるのだ。送信したステーションはコリジョン発生前に作業を終えているので、コリジョンに気づいていない。

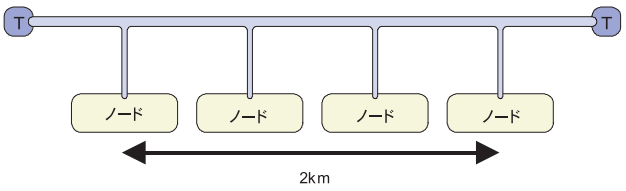


図 2-2　ネットワーク直径

こうした問題が潜んでいるため電気信号が銅のケーブルを通過するときの速度をもとに、Ethernet の最小フレームサイズが決められた。コリジョンが最も遠いポイントから戻って来て通過するのに十分な時間だけ送信モードのままで待機し、コリジョンを検出するようにしたのだ。Ethernet の規格では 512 ビット未満のデータパケットは伝送されない (これはリピーターとスイッチングのどちらにも、そして 10BASE と 100BASE のどちらにも共通した規格だ)。 512 ビット未満のデータパケットは自動的に引き伸ばされる。

Ethernet パケットの構成

Ethernet パケットの構成は図の通りだ。宛先として持たされるアドレスは受信する機器の MAC アドレスで、送信元アドレスは信号を送った機器の MAC アドレスだ (MAC アドレスについては後で紹介しよう)。

宛先のアドレス (6バイト)	送信元アドレス (6バイト)	プロトコル (2バイト)	ペイロード (46～1500バイト)	FCS (4バイト)

図 2-3　Ethernet パケット

プロトコルは IEEE が公に定めた数字からなる識別子で、受信側が待ち望むペイロードの種類を表している。たとえば CobraNet のIDは 8819 で、インターネット用の ID は 801 だ。

FCS はフレームチェックシーケンスの略で、1 ビットのデータが破損する可能性を 99.9%の確立で検知している。CRC と呼ばれることもある。

Ethernet の規格

Ethernet は 1980 年に IEEE 802.3 として規格化された。最初の規格は 50 Ω で 10mm の同軸を基準にしていたが、まもなくさまざまなバリエーションが登場した。

- 10BASE-5…いちばん最初の同軸ケーブルを使った Ethernet。
- 10BASE-2…10mm の代わりにより細い 5mm の 50 Ω同軸ケーブルを使ったもので、そのために「細い Ethernet」と呼ばれた。伝送速度は 10BASE-5 と同じ 10Mbps で最大ケーブル長は 185 メートルだ。標準的なT型 BNC コネクターを使い、ネットワークインタフェースカード (NIC) に 2 つあるコネクターを使ってデイジーチェーンで接続する。ケーブル 1 本で 30 台までのステーションを接続できる。
- 1BASE-2…10BASE-2 と同じだが伝送速度は 1Mbps だった。
- 10BROAD-36…ブロードバンドを実現した Ethernet。

この中で 10BASE-5 と 10BASE-2 だけが広く使われた。しかし今ではどちらも一般的ではない。

こうした初期の Etherne ネットワークはバックボーントポロジーと呼ばれるものを採用していた。単純に見えて広く使われたトポロジーだが同時に弱点でもあった。終端プラグが

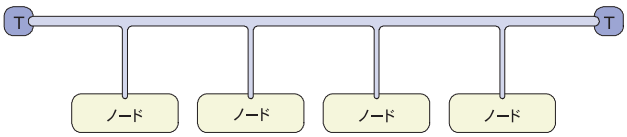


図 2-4　バックボーントポロジー

なかったり、あるノードとケーブルの接続に欠陥があるだけでネットワーク全体がダウンするのだ。つまり 1 点のトラブルで機能が停止してしまうのだが、最悪のシナリオはダウンした原因になったポイントを見つけ出すのが難しいことだ。

これを解決するにはバックボーンをなくすことだった。その結果バックボーントポロジーが変形してスタートポロジーになり、10BASE-T が誕生したのだ。

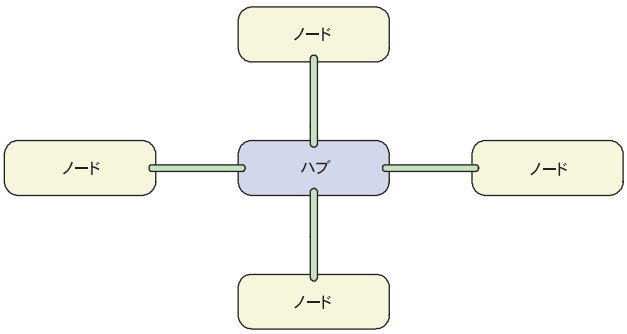


図 2-5　スタートポロジー

10BASE-T

10BASE- Tは 1990 年に登場した。同軸バックボーンの代わりに丈夫で安価なツイストペアケーブルとリピーターハブを使ったものだ。Ethernet そのものはまだメディアを共用するときにネットワーク直径の限界があった。パケット構造も同じままだ。各ステーションを接続するためには 2 ペアが必要だ。一方が入ってくるトラフィック用、もう一方が出て行くトラフィック用だ。各ステーションへ、あるいは各ステーションから伝送されたデータは中央まで帰ってくることになる。10BASE-T では、ネットワーク上で共用されるメディアの弱い部分を安全にしまい込み、オフィスの外にはまき散らさない。10BASE-T システムで配線障害が起きても、たいてい 1 つのステーションでネットワークサービスが停止するだけになった。

このトポロジーを使うと 1 つのスターを別のスターに接続できるため、より大きなネットワークが作れるようになった。図 2-6 にスター同士の接続を示したが、この中にはループがないことに注目していただきたい。ネットワークにループがあると、データが際限なく周りつづけて完全にネットワークをダウンさせる原因になるからだ。

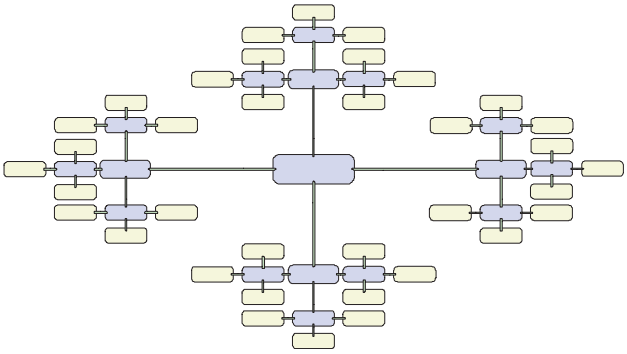


図 2-6　スターでスターを作る

このネットワークで使われる CAT3 ケーブルは最長 100m に制限されている。光ファイバーなら最大 2km のネットワークまでサポートされる。これが 10BASE-F と呼ばれるものだ。

100BASE Ethernet

100BASE Ethernet は最高 100Mbps(毎秒 100 メガビット) の速度でのデータ伝送をサポートしている。10 倍の速さでデータを伝送するためよくファスト Ethernet と呼ばれている。Ethernet と同様にファスト Ethernet も CSMA/ CDによるアクセスを採用しており、パケットのサイズや形式は 10BASE- X のグループと同じだ。10BASE からファスト Ethernet に代わってもビットレートが増えただけなのだ。いずれにしてもビット数が 10 倍だというのは今の伝送ラインにフィットしているのかもしれない。最小パケットサイズの必要条件を変えることもなく、むしろ正確にコリジョンを検出するためにネットワークの最大直径が小さくなった。ファスト Ethernet のリピーターネットワークでは最大直径を 200m に制限している。

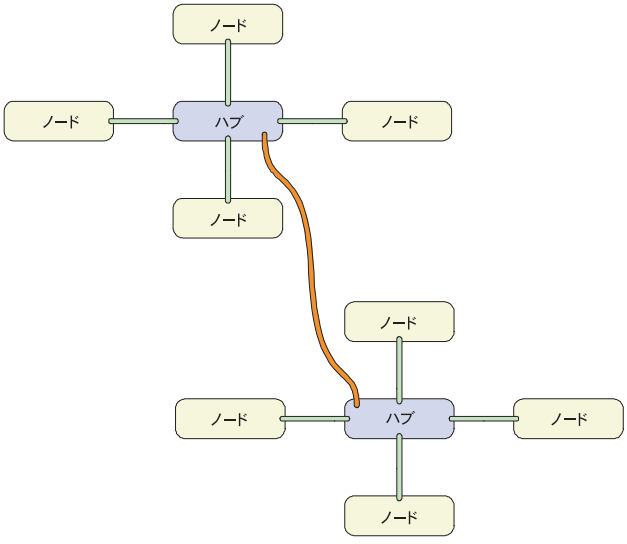


図 2-7　10BASE-F

ファスト Ethernet のバリエーション

Ethernet のようにファスト Ethernet にもさまざまなバリエーションがある。

- 100BASE-T4…CAT3 ケーブルの 4 対すべてを使ったファスト Ethernet。
- 100BASE- TX…CAT5 ケーブルの 2 対だけを使ったファスト Ethernet で最も広く使われているファスト Ethernet だ。
- 100BASE-FX…マルチモードファイバーを使ったファスト Ethernet。

ギガビット Ethernet

Ethernet 最新のものはギガビット Ethernet、または 1000BASE Ethernet と呼ばれるものだ。10BASE や 100BASE と同様にさまざまなバリエーションがありパケットの形式も同じだが、最小パケットサイズが大きくなっている。ネットワーク直径の限界は 200m のままだ。

200m のネットワーク直径を可能にするメカニズムはキャリア・エクステンションと呼ばれる。ギガビットネットワークアダプターが 512 バイト未満のフレームを伝送するときは常に、ギガビット MAC がキャリア・エクステンションと呼ばれる特殊な信号を送信する (この間中コリジョンを監視し続けている)。

Ethernet フレームとキャリアエクステンションによって最低でも 512 バイトになっても、送信時間は 100Mbps で 64 バイト送信するときと同じ程度だ。ギガビット MAC がこの期間内にコリジョンを検出すると通常のように反応し、ジャムシグナルを送信して攻撃的なステーションに一度活動を控えて後で再送信するよう指示する。

ギガビット Ethernet のバリエーション

- 1000BASE-SX…(S は shortwavelength の略だ) 光ファイバーケーブル用の光学式トランシーバーやレイヤーデバイスとして定義されている。マルチモードファイバーだけを対象にしていて、トランシーバーは長い波長をカバーするものに比べてさほど高価ではない。
- 1000BASE-LX…(L は long wavelength の略だ) 光ファイバーケーブル用の光学式トランシーバーやレイヤーデバイスとして定義されている。1000BASE - LX はマルチモードとシングルモードどちらかのファイバーを使うよう指定する。
- 1000BASE-LH…(LH は long haul の略) 多くのメーカーからトランシーバーが発売されているが、カバーする距離はメーカーによって異なる。IEEE の規格ではないが多くのメーカーが IEEE の 1000BASE-LX と相互機能するよう製造している。
- 1000BASE-T…CAT5 を使ったギガビット Etherne だ。4 対をすべて使い最長 100m までのばせる。

将来

無線 Ethernet、IEEE 802.11 が人気を集めていてもっと広く使われるようになるだろう。同じくメディアを共用しバンドワイズは 11Mbps だ。50Mbps のバージョンは開発途上だが、まもなく利用可能になるはずだ。

CAT5 ケーブルを使ってファスト Ethernet の機器に電源を供給することは多くのメーカーで実現している。これをどうやって基準化するか進行中なので、メーカーが違っても相互動作するようになるかも知れない。　Ethernet 上でインターネット・プロトコルを使って声を伝えるアプリケーション (Voice/IP) の1つが電話になるだろう。

Chapter 3　プロジェクトにふさわしいケーブルを選択する

はじめに

この章ではネットワークケーブルプラントを設計、設置する際の情報を提供しよう。高品質のネットワークを設備する手助けになるよう、ケーブルプラントについて考慮する事柄の概要を説明する。

ケーブルプラント

一般的な Ethernet ネットワークのケーブルパスは図の通りだ。ケーブルプラントを構成するアイテムは下記の通り。

- ノード同士を接続するケーブル…CAT5 や光ファイバーケーブル
- 配線クロゼットのパッチパネル
- ステーションケーブル…壁面パネルとノードを接続するケーブル
- 壁面プレート…ノードの近くにあるデータや情報のアウトレットポイント

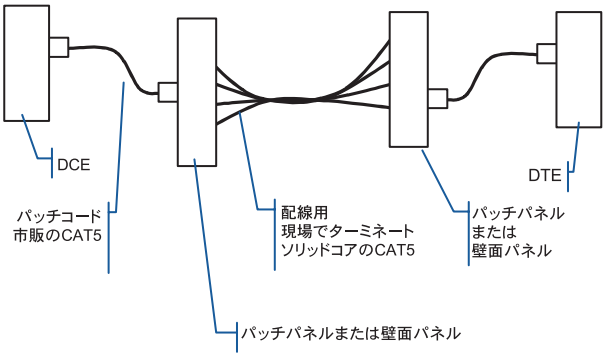


図 3-1　一般的なケーブルプラント

図のように間にパッチポイントがあると良いだろう。拡張したり構成を変更できるようケーブルプラントに柔軟性を持たせられるからだ。

音声ネットワークには 2 種類のケーブルが使われる。CAT5 と光ファイバーケーブルだ。以下にそれぞれに関連する事項を紹介しよう。

CAT5

CAT5 は安価でシールドされていないツイストペア (UTP) の通信グレードケーブルだ。どこででも見かける電話用ケーブルによく似ているが、各ペアはよりしっかりツイストされている。CAT5 はすべて UTP ではないことにも注意しよう。シールドされた (STP)CAT5 は価格が高く UTP の CAT5 より限界距離がかなり短い。

距離の限界

ファスト Ethernet システムでは CAT5 ケーブルの距離を 100m に制限しているが、これは信号の放射と減衰を考慮したためだ。100m を超えると電磁干渉 (EMI) を受けやすくなる。

コネクター

CAT5 ケーブルの終端は RJ-45 コネクターだ。RJ-45 には 2 種類ある。ソリッドコアの CAT5 に使うためのベントタイプと標準の CAT5 ケーブルに使うためコンタクトが直線に

なっているタイプだ。ケーブルとコネクターの組み合わせを間違うと問題が発生することもある。図 3-2 はモジュラーコネクターの 1 つのコンタクトの先端を示している。(左側の) 直線タイプは心線の中心が突き抜けるように接続するので標準のケーブルでしか使えない。曲がったタイプには数種類あり、コンダクタをまたがせるためにコンタクトが互いにオフセットしている。そのためソリッドタイプと標準のケーブルどちらでも使えるのだ。

モジュラーコネクターのケーブル開口部にもフラットケーブル用と丸いケーブル用の楕円形のものがある。CAT5 の場合は通常フラットケーブル用に作られたコネクターにはうまくフィットしない。安いモジュラーコネクタはコンタクトを金めっきなどせず金をフラッシュめっきしているだけだ。きちんとめっきしていないコネクターは摩耗が速いし腐食の可能性もあり、その結果接続の信頼性を低下させることになる。

AMP のモジュラーコネクターは高品質だが、2 つ目のクリンプポイントが他のメーカーと違う位置にある。図 3.4 が標準的なクリンプとAMPプラグの違いを表したものだ。A が1つ目のクリンプポイントで、ケーブルの外装にロックされるようリリーフタブを折りまげる。プラグの反対側ではコンタクトが各コンダクタに押し込まれる。B が2つ目のクリンプポイントで、コンタクトから抜け落ちないようにコンダクタを保護するものだ。

AMPのコネクターはこのクリンプポイントが他のメーカーと場所が違う。AMPのコネクターに標準のクリンパーを使うと、このクリンプがふさがったり曲がったり場合によっては壊れる。逆に標準的なコネクターにAMP用のクリンパーを使うとさいころが壊れることになる。しかしどちらの種類のプラグでも心線でクリンプしてしまえば交換できるし、どんなジャックにもきちんと差し込める。

プラグによっては心線を差し込むときのガイドが付いた物ものある。これなら簡単にきちんと配線できる。インサート付きのコネクターなら特性がより向上する場合がある。

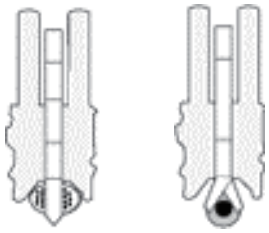


図 3-2　直線タイプとベントタイプ

図 3-3　開口部

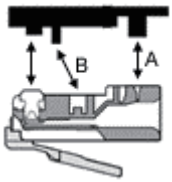


図 3-4　標準のクリンパーと AMP のプラグ

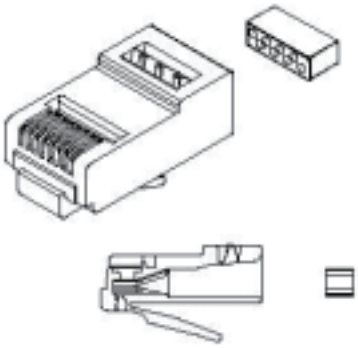


図 3-5　インサート付きプラグ

ツイストと終端

CAT5 ケーブルはツイストされた 4 対の心線でできている。1 対 (1 番ピンと 2 番ピン) が送信用、もう 1 対 (3 番ピンと 6 番ピン) が受信用だ。残る 2 対はターミネートされているが使わない。Ethernet では 4 対のうち 2 対しか使わないが、すべてのペアがターミネートされていてきちんとツイストされていることが重要だ。CAT5 ケーブルの配線とカラーコードを定義する規格は EIA/TIA の 568A と 568B、AT&T 258A だ。いずれも遠距離通信で使われる USOC の規格とは違う。

CAT5 UTP ケーブルをターミネートするとき各対ができるだけコネクター近くまで自然にツイストされていることが重要だ。EIA/TIA の規格 568B ではツイストされていない部分を

ピン	信号	EIA/TIA 568A	EIA/TIA 568B	Ethernet
1	送信 +	白 / 緑	白 / 橙	使用
2	送信 -	緑 / 白 or 緑	橙 / 白 or 橙	使用
3	受信 +	白 / 橙	白 / 緑	使用
4	N/A	青 / 白 or 青	青 / 白 or 青	未使用※
5	N/A	白 / 青	白 / 青	未使用※
6	受信 -	橙 / 白 or 橙	緑 / 白 or 緑	使用
7	N/A	白 / 茶	白 / 茶	未使用※
8	N/A	茶 / 白 or 茶	茶 / 白 or 茶	未使用※

※…未使用の心線もターミネートしておくこと

表 3-1　CAT5 ケーブルの配線とカラーコード

約 12.5mm 未満にするよう要求している。12.5mm 以上ツイストされていない部分があるとハイビットレートでの特性に影響を与えるだろう。

ストレートケーブル VS クロスケーブル

ネットワークで一般的に使われる CAT5 ケーブルには 2 種類ある。ストレートケーブルとクロスケーブルだ。違いはケーブルの終端でコンダクタがどうターミネートされているかだ。表は CAT5 のクロスケーブルとストレートケーブルでの RJ-45 の「ピンアサイン」を示している。

クロスケーブル	
RJ-45 ピン	RJ-45 ピン
1…受信 +	3…送信 +
2…受信 -	6…送信 -
3…送信 +	1…受信 +
6…送信 -	2…受信 -

ストレートケーブル	
RJ-45 ピン	RJ-45 ピン
1…受信 +	1…受信 +
2…受信 -	2…受信 -
3…送信 +	3…送信 +
6…送信 -	6…送信 -

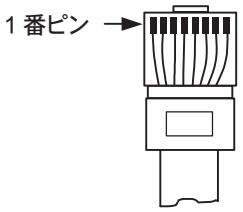


図 3-6　RJ-45 コネクターのピンアサイン

ストレートケーブルはスイッチングハブにネットワーク装置 (DTE) を接続するときに使われる。DTE やスイッチングハブと他のネットワークデバイスについては次の章で説明しよう。送信用のピンを直接ネットワークデバイスの受信用ピンに (つまり 1 番ピンと 1 番ピン、2 番ピンと 2 番ピン、というように) 接続することになり、逆もまた真だ。クロスケーブルはスイッチングハブ同士を接続するために使われる。クロスケーブルでは RJ-45 の一方でピンアサインが入れ替わっている (1 番ピンと 3 番ピン、2 番ピンと 6 番ピン、3 番ピンと 1 番ピン、6 番ピンと 2 番ピンが接続されている状態) ため、一方のスイッチングハブにある送信用のピンともう一方のスイッチングハブにある受信用のピンを接続できるのだ。

クロスケーブルとストレートケーブルを見分けるには、両端で RJ-45 コネクターのコンダクタを見れば良い。両端で配線が同じならストレートケーブルだし違っていればクロスケーブルだろう。

スイッチングハブによっては自動選択のクロスオーバー機能を持つものもある。どのポートにもストレートケーブルとクロスケーブルのどちらでも接続することができるというものだ。スイッチングハブがケーブルに合わせて自動で電気的に調整してくれる。

クロスケーブルとアップリンクポート

リピーターハブやスイッチングハブにはアップリンクポートを持つものがある。他のスイッチングハブやリピーターハブに接続するためのものだ。アップリンクポートはクロスケーブルの代わりにストレートケーブルで配線するためのものだ。ただしアップリンクポートが隣りのポートと接続を共用しているものがあるので、必ず取扱説明書で確認しておこう。

光ファイバーケーブル

光ファイバーには 2 種類ある。シングルモードとマルチモードで、両方ともは Ethernet ネットワークに使用できる。Ethernet で光ファイバーケーブルを使うとき、2 つの接続が必要だ。一方が送信用、もう一方が受信用だ。

マルチモードファイバーは 2 種類のガラスを同軸にアレン

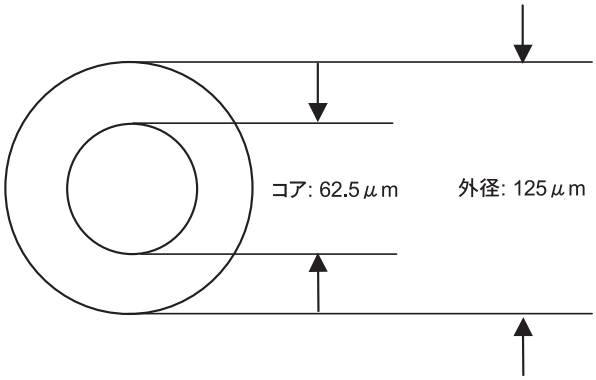


図 3-7　マルチモードファイバー

ジしたものだ。その名の通り、光ファイバーが通過するためのモード (パス) をたくさん持っている。コアが比較的大きいので手ごろな価格の LED を光源にできるし、カプラーやコネクターもさほど高価ではない。

マルチモードファイバーには 2 つのサイズがある。主にデータ通信用の 62.5 / 125 μm、そして主に遠距離通信用の 50/100 のμmだ。62.5 / 125 μmマルチモードファイバーを使った 100Mbit Ethernet の規格は 100BASE-FX と呼ばれている。100BASE-FX はの限界距離は 2km だ。

シングルモードの光ファイバーケーブルは 1 種類だけのガラスでできている。コアは8から 10 μ m で、8/125 のμmが最も一般に使われている。このケーブルには光のパスが 1 つしかない。

ケーブルの価格はマルチモードとほぼ同じだが、送信機や受話器がマルチモードよりかなり高価だ。シングルモードファイバーのコア直径はかなり小さいので光が通過できるパスは 1 つだけだ。このためバンドワイズの限界はなくなるが、ファイバーに光をカップリングが難しくなる。

マルチモードファイバーの限界距離は 2km だが、シングルモードファイバーの限界距離は使用するシステムによって変化する。いずれにしても 2km は超える。現在シングルモードファイバーを使った Ethernet の規格はない。

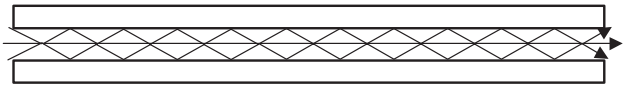


図 3-8　マルチモードファイバーの光のパス

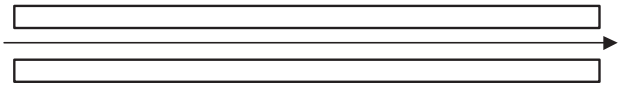
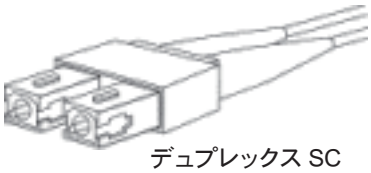


図 3-9　シングルモードファイバーの光のパス

コネクター

光ファイバー用のコネクターには 2 つ種類がある。SC と ST だ。ST はストレート・チップの略で光ファイバーで最も広く使われているが、Ethernet ではもはや使われなくなった。BNC コネクターによく似たバレル型のコネクターで AT&T が開発したものだ。今では新しい SC の方がより広く使われている。限られたスペースでも簡単に接続できるよう四角い。スイッチングハブのファイバーモジュールにはたいてい SC が付いていて 100Mbit とギガビットを選択するコネクターになっている。SC にはデュプレックスタイプもあり、送信側と受信側を間違って接続するのを防止してくれる。

今後さらに多く見かけるようになる可能性のあるファーバー用のコネクターが2つある。MTRJ と MTP だ。どちらもデュプレックスで RJ-45 と同じ程度の大きさだ。



デュプレックス SC

図 3-10　光ファイバー用コネクター

配線とネットワークの特性

Ethernetネットワークの特性を劣化させる要因は多く、ケーブルプラントの貧弱さもその 1 つだ。配線に問題があってEMI の影響を受けやすくパケット損失の原因になることもある。ここでは配線について考慮すべき点を挙げるので高品質ケーブルプラントを設備する手助けにしていただきたい。

音声の配線に似てネットワークケーブルの配線を設計するときにも、気をつけるべき仕様に近いものがある。CAT5 の

およそのガイドラインをいくつか表にまとめた。光ファイバーケーブルの場合はもともとEMIやRFIへの耐性があるため、こうしたガイドラインを考慮する必要はない。

状態	2kVA 未満	2 - 5kVA	5kVA 超
シールドしていない電源コードや機器とコンジットのない非金属の配線経路	12.7cm	30.5cm	61cm
シールドしていない電源コードや機器と接地した金属製コンジットのパス	6.4cm	15.2cm	30.5cm
接地同等の処理を施した金属製コンジット内に配線された電源コードと接地した金属製コンジットのパス	N/A	15.2cm	30.5cm
トランスや電源モーター	1.02m	1.02m	1.02m
蛍光灯	30.5cm	30.5cm	30.5cm

表 3-2　およそのガイドライン

CAT5 とケーブルタイ

設備の品質を劣化するもう 1 つの要因がきっちり巻かれたケーブルタイだ。UTP ケーブルの外装を傷つけるほどタイを締め付けてはいけない。タイの下でケーブルのインピーダンスがわずかに変わりネットワークの特性を低下させるからだ。等間隔にタイでケーブルをきつく縛ることになれば特性はさらに低下する。

引く力と曲げるときの半径

光ファイバーケーブルが壊れやすいというのは作り話だ。実際、光ファイバーの伸張力は同じ直径の銅やスチールファイバーより強い。柔らかいし簡単に曲げられるし、銅ケーブルとは違って腐食にも強い。光ファイバーケーブルは 150 ポンド以上もの引張力に耐えられる。実際には CAT5 の方が光ファイバーケーブルより壊れやすいかもしれない。ケーブルタイできつく巻いた部分、コネクター付近のツイストされていない部分、急な角度で曲げた部分はケーブルの特性が低下してカテゴリ5の特性要求を満たせなくなる場合もある。光ファイバーケーブルが壊れやすいというのは実際よりも大げさだが、もちろん限界はある。だから CAT5 と光ファイバーケーブルのどちらも設置の際には注意を払わなければならない。ここで CAT5 と光ファイバーケーブルを曲げるときの半径と引張力の概要を紹介しよう。

CAT5 の場合

UTP ケーブルが耐えられる引張力は音響業界で考えられている数値よりもかなり低い。設置作業中に 25 ポンド以上の力をかけるともはや仕様を満たさなくなる場合もある。音声ケーブルの場合と同じように UTP ケーブルを曲げるときは最小半径という限界がある。一般的な CAT5 はケーブル直径の 4 倍が曲げるときの最小半径だ。ケーブル径が 1/4 インチなら 1 インチが限界になる。メーカーが指定していない場合はこれをガイドラインにすればかなり安全だろう。ただし最小直径ではなく最小半径なのでご注意のほど。

光ファイバーケーブルの場合

光ファイバーケーブルを曲げるときの半径と引張力の限界は、使用しているファイバーの種類と数によって大きく異なる。曲げるときの最小半径が指定されない場合はケーブル外径の 10 倍を考えればたいてい安全だ。引張力はおよそ 50 ポンドから 150 ポンド以上までの範囲になるだろう。ふだんは使用するケーブルのメーカーに仕様を問い合わせるよう勧めている。

Chapter 4　プロジェクトにふさわしいハードウェアを選択する

はじめに

ネットワークを構成するアイテムには 3 つの分類がある。

・ケーブルプラント
・データ端末装置 (DTE)
・データ通信装置 (DCE)

図で点線になっているものがネットワークケーブルプラント、グレーになっているのがデータ端末装置だ。この場合 Ethernet スイッチングハブがデータ通信装置になっている。ここではデータ端末装置も紹介するが、主にデータ通信装置に焦点を合わせる。

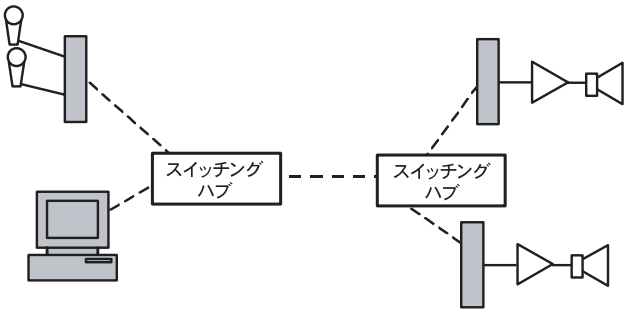


図 4-1　音声ネットワーク

データ端末装置

データ端末装置とはネットワーク上でデータを生成したり消費する装置のことだ。ネットワークノードと呼ばれることもあり、パソコンやネットワークプリンターが含まれる。CobraNet デバイスや他の「ネットワークで結ばれた」音声デバイスもデータ端末装置だ。音声ネットワークデバイスについては後でより詳しく紹介しよう。

データ通信装置と Ethernet ハードウェア

データ通信装置はワークグループ機器や相互接続用のコンポーネントに分類される。ワークグループ機器にはリピーターハブやスイッチングハブのようなデバイスが含まれ、相互接続用のコンポーネントにはルーター、ブリッジ、コアスイッチが含まれる。

ネットワークインターフェースカード

NIC ことネットワークインタフェースカードは、パソコンをネットワークに接続してアクセスさせるためのものだ。NIC はレイヤーを特定するため、AppleTalk の NIC を搭載しても Ethernet ネットワーク上では機能しない。

リピーターハブ

リピーターハブはマルチポートの Ethernet デバイスだ。信号を受信するとクロックを直してブーストし、すべてのポートに送信する。音声の世界で言えば「ミックスマイナス」システムだ。ポートの受信ペアに到着したデータ信号シグナルを電気的に再発振し、送信ペアから他の全ポートへ送り出す。その結果、リピーターハブを使ったネットワークはスタートポロジーでしか配線できないことになる。環状トポロジーを使うとデータがいつまでも回り続けることになるからだ。

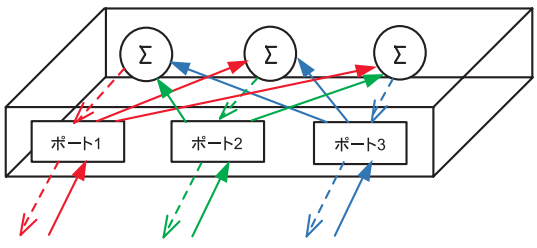


図 4-2　リピーターハブ

リピーターハブが受け取ったデータはネットワーク上すべてのデバイスに送られるため、リピーターネットワークはバンドワイズを共用しなければならない。バンドワイズは一定時間内に伝送できるデータ量を毎秒メガビット (Mbps) で表したものだ。ファスト Ethernet ネットワーク上でリピーターハブを使うとき、ネットワーク全体で利用可能なバンドワイズは 100Mbps だということになる。

リピーターハブはハーフデュプレックスモードで機能する。つまりデータの送信と受信を同時にできないのだ。またリピーターネットワークはコリジョンドメインだと考えられる。コリジョンドメインはハーフデュプレックスの Ethernet システムで、その要素はすべて同じタイミングドメインに存在する。つまり 1 つのリピーターネットワーク上で複数のデバイスが同時に送信しようとするとコリジョンが発生するのだ。こうなるとどのデバイスも送信を停止して適当な時間だけ待機し、それからデータを再送信しようとする。コリジョンドメインの各デバイスにそうさせるためにはプロトコルが必要だ。

・利用可能なネットワークのバンドワイズを共用する
・1 つのデバイスが送信している状態を検出する
・コリジョンの発生を検出する

使われるプロトコルは CSMA/ CD、Carrier Sense Multiple Access with Collision Detect という名で知られている。Ethernet ネットワークには指定された「管制塔」がないため各デバイスが独立して稼働しなければならない。そこで CSMA/ CDプロトコルが各デバイスに同じルールを適用し、共用メディアに接続したすべてのステーションを協力させるのだ。

Ethernet ネットワーク上では信号がかなりの速度で伝送されるが、それでもネットワークすべてを通過するにはある時間が必要だ。ケーブルが長いと信号がシステムの端から端まで移動するための所用時間も長くなる。CSMA/ CDがきちんと機能するためには、最大ケーブル長とネットワーク直径の限界を設けなければならない。ネットワーク直径はネットワーク上で 2 つのデータ端末装置を接続する最も長いケーブル長で決まる。最高 2 つのハブと受話器を通過する時間の余裕を見て、ファスト Ethernet のリピーターネットワークでは一般的に 200m 程度が最大ネットワーク直径になる。

ネットワークの設計者や管理者は早くもリピーターハブを捨てている。スイッチングハブの価格が劇的に下がったからだ。このためここでもスイッチングハブを利用したネットワークに焦点を合わせることにする。

スイッチングハブ

スイッチングハブは Ethernet のブリッジングテクノロジーに基づき、ネットワーク上のデバイス間にあってデータパケットにフィルターをかけたり転送したりするマルチポートのデバイスだ。リピーターハブとは異なり、スイッチングハブは各

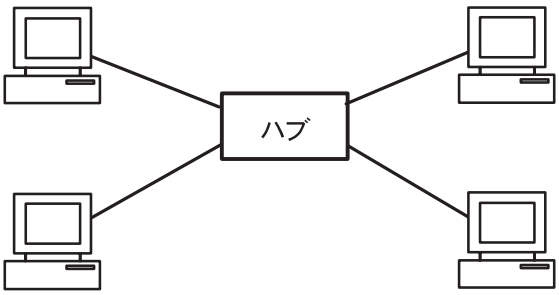


図 4-3　スタートポロジー

コンポーネント	通過時間 (ビットピリオド)
光ファイバー (マルチモード / シングルモード)	1.000/m
CAT5 ケーブル	1.112/m
レシーバ	100 以上
クラス 1 リピーターハブ	140 以上
クラス 2 リピーターハブ	92 以上

表 4-1　ネットワークコンポーネントの通過時間

データパケットの宛先アドレスを読んで正しいポートに転送することができる。この知能のおかげでパケットに指定された所定のデバイスだけがデータを受信するのだ。

もう１つのメリットはスイッチングハブが同時に受信・送信するということだ。スイッチングハブはフルデュプレックスのデバイスで、各ポートが独立して稼働する。たとえば100Mbps のネットワークなら各ポートが同時にそれぞれの方向に 100Mbps でデータを処理できるのだ。つまり１つのリンクで 200Mbps のバンドワイズを提供することになる。スイッチングハブ同士のリンクにはまだバンドワイズの限界はあるが、１つのスイッチングネットワーク中で利用可能なバンドワイズの合計はかなり大きくなる。スイッチングハブを追加すればネットワーク全体のバンドワイズは簡単に増やせるのだ。

スイッチングハブの各ポートがフルデュプレックスで独立して稼働しているため、コリジョンが発生することはない。そのためリピーターハブで使われていた CSMA/ CDプロトコルはいらない。つまりネットワーク直径の限界がなくなり、より大きなネットワークを構築できるのだ。

リピーターネットワークではコリジョンドメインを分割するためにスイッチングハブを使っていた。スイッチングハブはコリジョンの通過を妨げながら、データを別のコリジョンドメインへ渡せるからだ。

スイッチングハブならギガビット Ethernet と ATM のような異なるネットワーク同士やスピードの違う LAN を接続することもできる。

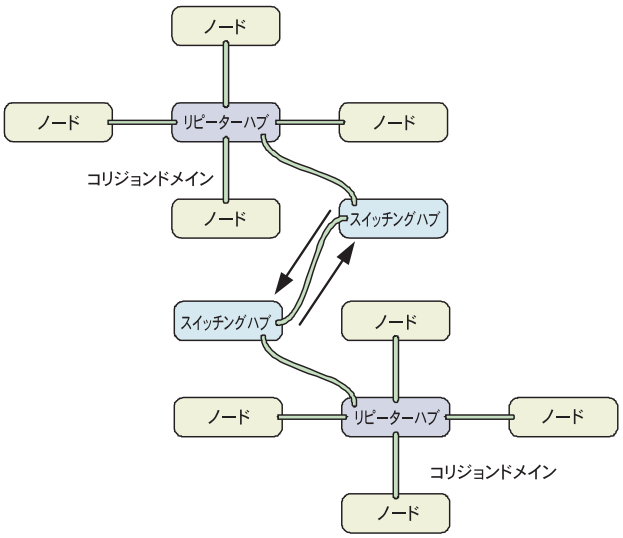


図 4-4　フルデュプレックス

スイッチングハブはどう機能しているのか

スイッチングハブは 4 つの主な部分から構成されている。

- ポート
- ルックアップテーブル (LUT)
- FIFO列
- スイッチファブリック

スイッチングハブのポートはフルデュプレックスモードで個別に稼働し、複数のポートで同時に通信を続けられる。このためネットワーク上で利用可能なバンドワイズの量を増やすだけではなく、スイッチングハブをリピーターハブより効率的なものにしているのだ。

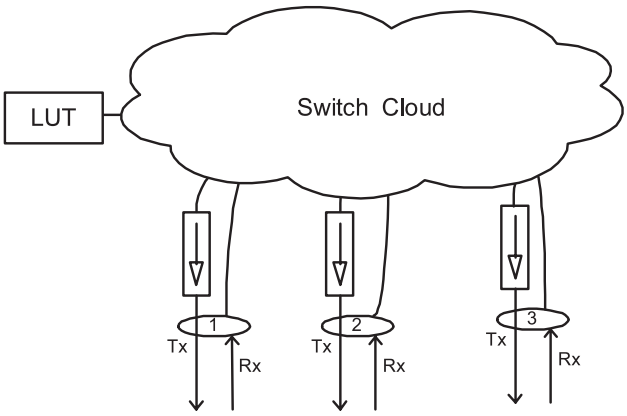


図 4-5　スイッチングハブ

ルックアップテーブル (LUT) はパケットを選ばれたポートにだけ送るためのものだ。ルックアップテーブルには各ポートのリストとそこに接続しているデバイスの MAC アドレスが入っている。Media access control address、略して MAC アドレスはネットワーク上で各ノードを識別するため IEEE が決めたハードウェアのアドレスだ。ネットワークノードがパケットを送るとき、スイッチングハブは入ってくる各パケットの送信元 MAC アドレスを読む。そのアドレスがルックアップテー

ブルになければ追加する。後でそのデバイスに向けてデータが送られて来たとき、スイッチングハブはその送り先を知っていることになるのだ。しばらくの間にスイッチングハブは各ポートに接続された全デバイスの MAC アドレスを学習する。

スイッチングハブは忘れてしまうこともできる。あるアドレスから一定時間 (たいてい 5 分間) パケットが送信も受信もされないとき、あるいは突然別のポートで発見されたアドレスはルックアップテーブルから削除される。これならノードを自由に移動できるという柔軟性が生まれるし、ルックアップテーブルが誤った情報を持っている心配もない。

スイッチングハブはまた、アドレスの種類を区別する能力も持っている。

- 入って来たパケットの宛先アドレスがユニキャストアドレス (1 対 1) の場合は、そのデバイスが接続されたポートにだけ送られる。
- 入って来たパケットの宛先アドレスがマルチキャストアドレス (1 対多) の場合はすべてのポートに送られる。

宛先アドレスがルックアップテーブルにない場合はすべてのポートに送られる。フラッディング (洪水) と呼ばれる現象だが、これで未知の宛先アドレスを持ったパケットが正しいノードに届くことを保証しているのだ。

FIFO 列は first-in-first-out、つまり「最初に入ったものが最初に出て行く列」という意味だ。各ポートには短期間のバッファメモリがある。パケットはここで待ち行列に入るので、スイッチングハブは 1 つのデバイスに向けられた多数のパケットを送信処理できるのだ。

スイッチファブリックは、パケットデータをスイッチングハブのあるポートの入力から単数ないし複数のポートの出力に移動する手段だ。ルックアップテーブルとスイッチファブリックは共同でパケットをスイッチングハブの中でルーティングしている。パケットの宛先はルックアップテーブルが知っていて実際にはスイッチファブリックが届けてやるのだ。

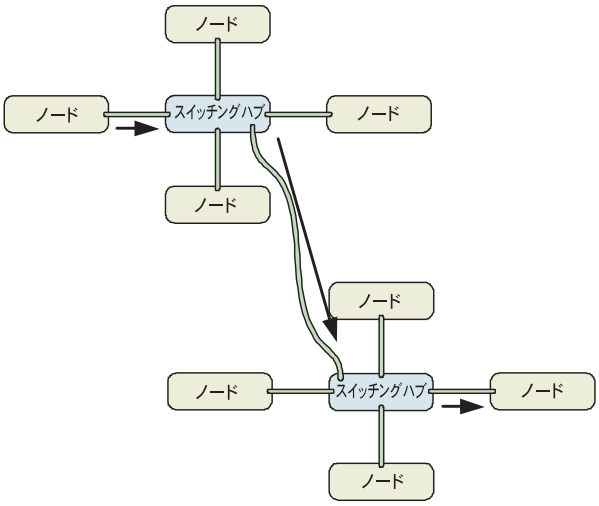


図 4-6　ユニキャストアドレス

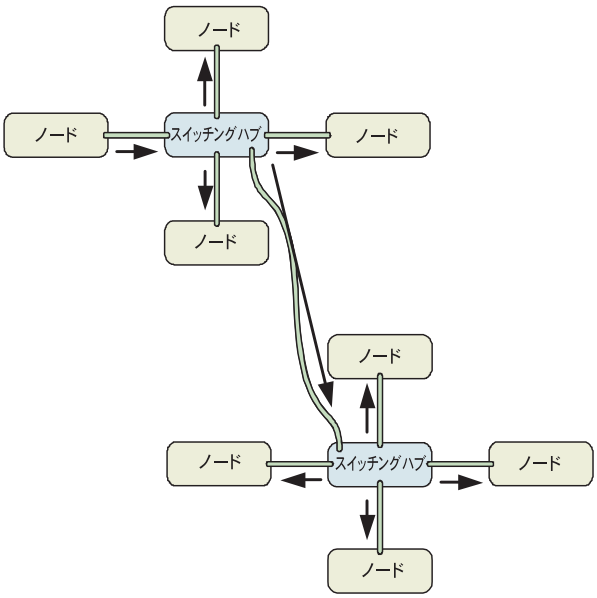


図 4-7　マルチキャストアドレス

管理機能を持つスイッチングハブ VS 管理機能を持たないスイッチングハブ

スイッチングハブには管理機能を持つものと持たないものがある。管理機能のないスイッチングハブはプラグアンドプレイで、場合によっては設定オプションがわずかに付いている。管理機能を持たないスイッチングハブの設定はたいてい DIP スイッチで行なう。

管理機能を持つスイッチングハブは、スパニングツリープロトコル、リンクアグリゲーション、メッシュのような故障に強い設定を行うためのオプションをはじめ、かなり多くの設定変更オプションを持っている。管理機能を持つスイッチングハブはスイッチングハブ自身の動作、トラフィックの状況、

バンドワイズの利用状況、ポート構成の状態など分析やトラブルシュートに役立つ情報をネットワーク管理者に提供する。こうした設定変更用のインタフェースにはたいていウェブブラウザや Telnet が使われる。進歩的なネットワークに関するトピックは後で紹介するが、いずれも管理機能を持つスイッチングハブでだけ利用できる。

スイッチングネットワークのトポロジー

スイッチングネットワークはリピーターネットワークに似たスタートポロジーで配線される。リピーターハブをスイッチングハブに置き換えれば、ネットワーク全体で 100Mbps だったバンドワイズがリンクあたり各方向に 100Mbps へと増えることになるのだ。

スイッチングハブは環状に接続することもできるが、ループ状態を防止するプロトコルをサポートしたスイッチングハブを使うことが条件だ。スパニングツリープロトコル、リンクアグリゲーション、あるいは HP 専有のメッシュといったプロトコルだが、いずれも管理機能を持つスイッチングハブにだけ利用可能だ。

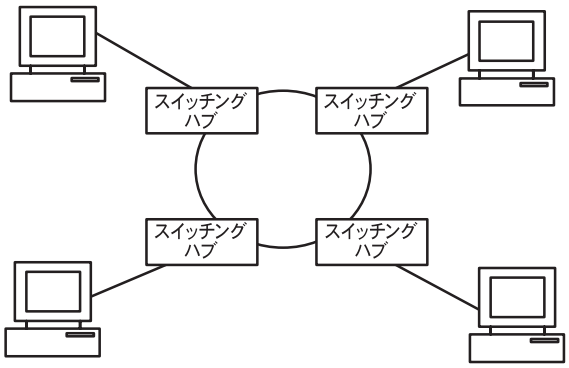


図 4-8　環状トポロジー

リピーターハブ対スイッチングハブ

ここ数年の劇的な価格低下によって、スイッチングハブを使わない理由はなくなった。スイッチングハブならノード同士の距離が長い大きなネットワークを構成できるし、故障に強いネットワークを構築することもできる。チャンネル許容量も増えるし、さらにギガビットのようにより大きなチャネル許容量に対応することもできる。

ブリッジとルーター

ここでは音声ネットワークにスイッチングハブを使うことに焦点を合わせているが、相互接続コンポーネントに関する情報も有意義だろう。

ルーターとは LAN を接続するものだ。プロトコルに依存してはいるが、同じレイヤー 3 プロトコルを使って LAN を接続するものであり、レイヤー 2 からは独立していてある種のポート (Ethernet、トークンリング、ISDN など) を装備していることも多い。ルーターはまず受信したすべてのパケットからレイヤー 2 ヘッダーを消し、レイヤー 3 ヘッダーを調べてそのパケットをどうルーティングするか決める。それから宛先のレイヤーに合わせて新しいレイヤー 2 ヘッダーを生成してパケットを送る。

ブリッジも同じように LAN を結ぶために使う 2 ポートのデバイスだ。ブリッジはプロトコルに依存せずレイヤー 2 でだけ機能する。ブリッジはただ Ethernet パケットを見るだけでパケットが運んでいるレイヤー 3 プロトコルのことなど気にもかけない。パケットを分析しないのだ。ただデータを転送するだけなのでルーターより処理は速い。Ethernet スイッチ

ングハブもブリッジングテクノロジーを基本にしているので、かつては「マルチポートブリッジ」と呼ばれていた。しかし近年スイッチングテクノロジーがかなり発達したため、ブリッジはそれほど一般的ではなくなった。現実に今ではブリッジを「2 ポートのスイッチングハブ」と呼ぶことさえあるのだ。

リンクを確立する

音声信号を長距離にわたって伝送する、EMI の耐性を高めたい、既存のコンジットにケーブルを通すスペースがない、などさまざまな理由でネットワークに光ファイバーが使われている。優れた設計のためには、スイッチングハブ、リピーターハブ、メディアコンバータのようなネットワークデバイスがどのように相互作用しているかを理解することが重要だ。

10Mbps ネットワーク

10Mbps のネットワークデバイスはデータを送信していないとき送信ラインをアイドル状態にする。一定期間内にデータ伝送が再開されなければそのデバイスはノーマルリンクパルス (NLP) を送信し始める。データを伝送していない 10Mbit のデバイスがネットワーク上にあることを他のデバイスに認識してもらう (つまりリンクを可能にする) ために送信するのだが、10Mbps デバイスと 100Mbps デバイス、あるいは 10/100 デバイスから区別するためにも役立っている。

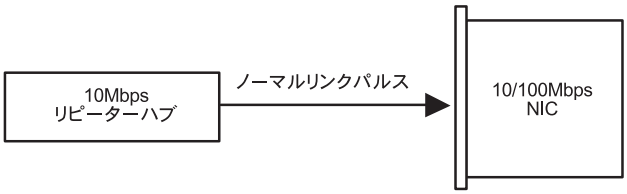


図 4-9　ノーマルリンクパルス

100Mbps デバイス

10Mbps のデバイスとは異なり、100Mbps のデバイスはデータを送信していないときでも活動を表明している。この活動はキャリアーと呼ばれ、100Mbps デバイス特有のものだ。

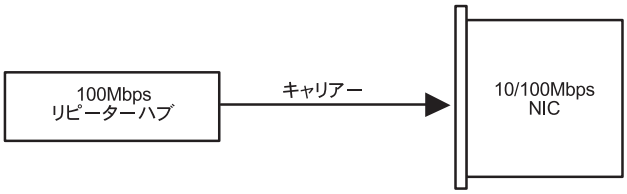


図 4-10　キャリアー

オートネゴシエーションするデバイス

リンクを確立する前に、CobraNet デバイスや一般的なネットワークデバイスはオートネゴシエーションと呼ばれるプロセスに入る。オートネゴシエーションはビットレートの低い形式の通信だが、他のデバイスに対してフルデュプレックスとハーフデュプレックスのどちらなのか、あるいは 10Mbps、100Mbps、ギガビットのいずれなのかを表明するものだ。この情報はメッセージを形成するために集めたノーマルリンクパルスの配列、ファストリンクパルス (FLP) で伝えられる。

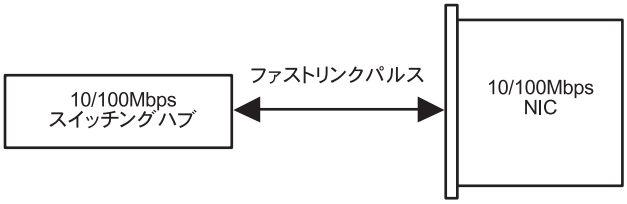


図 4-11　オートネゴシエーション

オートネゴシエーションの結果 10Mbps で接続されれば、ネットワークデバイスはアイドリングしているとき NLP を発信する。100Mbps で接続されればキャリア信号が発信される。

オートネゴシエーションできる任意のデバイスはパラレル検出も実行する。パラレル検出はネゴシエーションはせず、ファストリンクパルスを検出すると固定した速度でリンクを確立する。図は異なる能力のデバイス間でネットワーク接続が

どのように確立されているかを示したものだ。フルデュプレックスのリンクではデバイスがパラレル検出できないことに注目してほしい。光ファイバーケーブルがオートネゴシエーションしないことも重要だ。光ファイバーではキャリア信号を使ってリンクを確立するが、フルデュプレックスで接続するなら手作業で設定しなければならない。

オートネゴシエーションの例

図 4.9 の例では 10/100 の NIC が 10Mbps のリピーターハブにつながれている。NIC は 2 種類のビットレートに対応しているため、どちらにするかを決めなければならない。接続するとき 10Mbps のリピーターハブがノーマルリンクパルスを発信し始める。10/100 の NIC はこのパルスを見て、相手が 10Mbps でハーフデュプレックスだ (ご記憶だろうか、リピーターハブハーフデュプレックスだ) ということを悟る。そして 2 つのデバイスでリンクが確立するわけだ。

図 4.10 でもまた NIC がリピーターハブに接続する速度を決めなければならない。デバイス同士をケーブルで接続すると 100Mbps のリピーターハブはキャリア信号を発信する。10/100 の NIC はキャリア信号を見て 100Mbps のハーフデュプレックスで接続するに違いないと認識する。それからリンクが確立する。

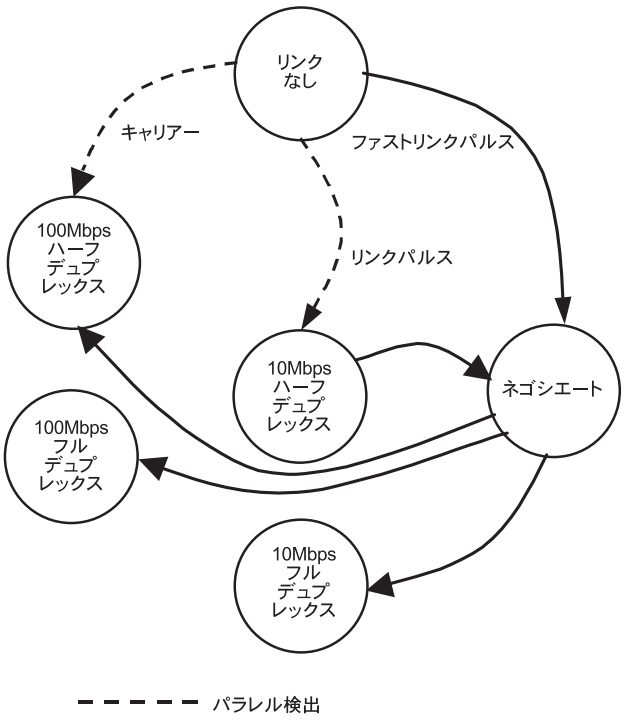


図 4-12　リンクステータスダイアグラム

メディアコンバータ

メディアコンバータは本質的にある形式のメディアを受け入れて別の形式に変換する 2 ポートのリピーターハブだ。最も一般的なのが光ファイバーと銅を変換するものだ。音声ネットワークにメディアコンバータを使うという目的で分類してみよう。

1. シンプルなメディアコンバータ
2. インテリジェント・メディアコンバータ

シンプルなメディアコンバータには知性がない。ただ光を電気のパルスに変換するだけだ。シンプルなメディアコンバータはファストリンクパルスを通すことも検知することもできないので、オートネゴシエーションできない。つまりオートネゴシエーションするデバイスと自分自身のリンクを確立する能力がないのだ。

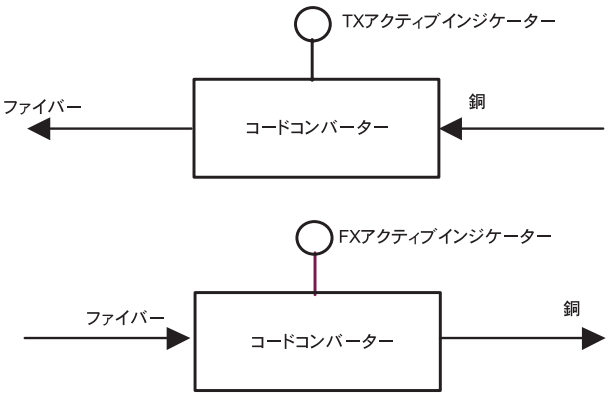


図 4-13　シンプルなメディアコンバーター

シンプルなメディアコンバータとは異なり、インテリジェント・メディアコンバータはファストリンクパルスを生成するし解釈することもできる。メディア変換に必要なエレクトロニクスの他に「ネゴシエーション」ブロックがあって、下記の特徴を持っているのだ。

- 接続速度をオートネゴシエーションか手作業で設定できる
- フルデュプレックスとハーフデュプレックスのどちらでも動作できる

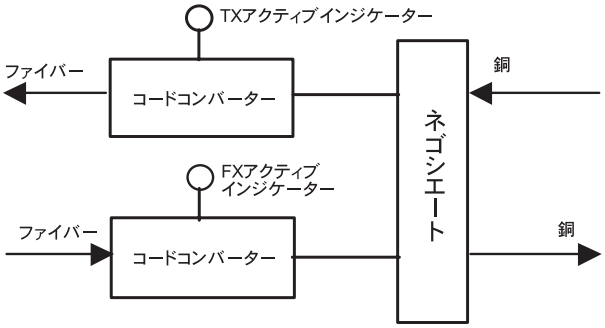


図 4-14　インテリジェントメディアコンバーター

ネットワークアドレスをアサインする

MAC アドレスはすべての Ethernet デバイスに割り当てられた個体識別用で重複しないアドレスだということはすでに紹介した。TCP/IP プロトコルはよりレベルの高いネットワークプロトコルで、IP アドレスと呼ばれる独自のアドレスシステムを持っている。では TCP/IP データが持つ独自のアドレススキームは、Ethernet や MAC アドレスにどう関連してくるのだろうか。

Ethernet パケットはネットワークプロトコル情報を搭載したペイロードを伝送している。TCP/IP も他のネットワークプロトコルと同じように、独自のアドレススキームとデータ構造を持っている。このため Ethernet ペイロードの中には他のフィールドが一式含まれていて、その中に TCP データと共に IP ソースや宛先アドレス情報をのせている。伝送されるプロトコルを定義し終わるまで Ethernet ペイロードの中に「巣を作り」続けるのだ。

これを理解する上で最も重要なことは、使っているネットワークプロトコルが完全に Ethernet から独立しているということだ。Ethernet はただの配送システムであり、ペイロードに入れて運んでいるネットワークデータにはお構いなしだ。つまり Ethernet では同じネットワーク上で多くの異なるネットワークプロトコルを運べることになる。データ端末装置上で起動しているネットワークソフトウェアまで運ばれたものを知りたければ、Ethernet のペイロードフィールドからネットワークプロトコル情報を抽出して見ればいい。

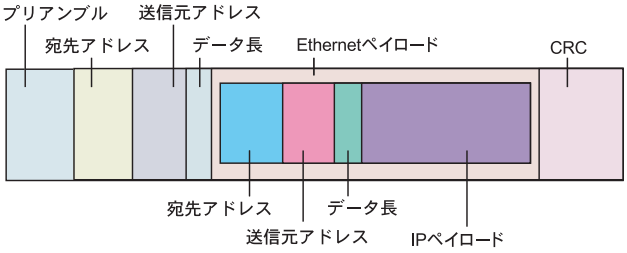


図 4-15　IP データを運ぶ Ethernet パケット

IP アドレス

IP アドレスは TCP/IP ネットワーク上でデバイスに割り当てられた重複しない識別用アドレスだ。独立したネットワークの中では各アドレスが重複していない限り任意に IP アドレスを割り当てられる。しかし私的なネットワークを直接インターネットに接続するときは IP アドレスの重複を避けるために (インターネットアドレスと呼ばれる) 登録された IP が必要だ。

IP アドレスは「ドットで区切られた 10 進法」で書かれた 32 ビットの数字によるもの (それぞれ 8 ビット× 4 パートに分かれている) だ。それぞれの区切りには 0 から 255 までの数字を入れられる。アドレスは 2 つの部分、ネットワークナンバー (今日ではネットワーク・プレフィックスと呼ぶ方が多くなってきた) とホストアドレスから成り立っている。ホストアドレスはネットワークノード独自のアドレスであり、ネットワークナンバーはそのホストが所属するネットワークを表すものだ。同じネットワークに接続しているホストのネットワークナンバーはすべて同じだが、ホストアドレスは他のデバイスと重複してはならない。同じようにネットワークナンバーが違えば 2 つのホストに同じホストアドレスをつけることができる。

IP アドレスが　192.168.2.0　の場合
2 進数にすると
11000000.10101000.00000000.00000010

図 4-16　IP アドレス

ネットワークナンバー	ホストアドレス

図 4-17　IP アドレスの形式

InterNIC はもともとインターネットアドレスを 3 クラスに分け、各クラスの境界をネットワークナンバーの間で固定してやり、ホストアドレスは 32 ビットのアドレスの別のポイントに表示させていた。これが「クラス分け」アドレスというやつだ。

- クラスA…1 千 6 百万のホストを接続する
  127 のネットワーク
  (1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx)
- クラスB…6 万 5 千のホストを接続する
  1 万 6 千のネットワーク
  (128.0.xxx.xxx ～ 191.255.xxx.xxx)
- クラスC…254 のホストを接続する
  2 百万のネットワーク
  (192.0.0.xxx ～ 223.255.255.xxx)

残念なことに誰もこれほど速くインターネットが普及するとは予想しなかったので、この方法でアドレスを割り当てるとどれほど制限が多く融通がきかないかまでは考えていなかった。そこでもう 1 つのアドレス階層であるサブネットを追加して、一時的に多くの欠点を克服している。

サブネットとサブネットマスク

サブネットはネットワーク中でプレフィックスを共有する要素だ。さらにアドレスのホスト部分を分割できるようにする。以前は新しいネットワークを構築する前に、インターネットからネットワーク番号を求められたものだ。

ネットワークをサブネットに分けられるときはサブネットを識別するためにホストアドレスの一部を使う。図 4.16 に示された IP アドレスを使って例を見てみよう。

ネットワークナンバーは

192.168.0

2 進数では

11000000.10101000.00000000

になる。そしてホストアドレスは

2

2 進数では

00000010

になる。

このネットワークを 13 のサブネットに分ける場合、ホストアドレスの最初の 4 ビット (0000) をサブネット認識用にリザーブする。サブネットは2の累乗の固まりでしか作れないので、この場合は16のサブネットを作ることになる。ホストアドレスの最初の 4 ビットを、サブネットナンバーを示すように変えることができる。

nnnn0010

ネットワークをサブネットに分けたら IP ノードは拡張されたネットワークナンバーとホストアドレスがどこで分割されているか知っていなければならない。そのためにサブネットマスクを使う。サブネットマスクはネットワークナンバーと、サブ

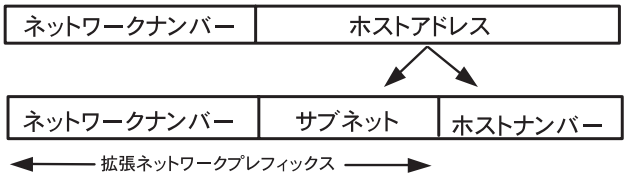


図 4-18　サブネットアドレスの形式

ネット認識用にリザーブされたビットを足したものだ。サブネットマスクを生み出すためには、新しいサブネットナンバーを含めたネットワークナンバー用のビットはすべて 1 になる。ここで取り上げている例で、サブネットマスクは

11111111.11111111.11111111.11110000

または　255.255.255.240.

クラスレスアドレス

インターネット上で使われた「クラス分け」アドレスは、今では CIDR、Classless Inter-Domain Routing と呼ばれるサブネットを基本にしたルーティングに置き換えられた。CIDR はクラスA、B、Cといったアドレスを排除し、拡張ネットワークプレフィックスというコンセプトに置き換えている。CIDR 用の標準のシンタックスは点をドットで区切った 10 進数で表記され、その後にスラッシュをつけてプレフィックスのビット数を書く。注釈にプレフィックス長を含めることでホストの構成を設定するとき IP アドレスやサブネットマスクを指定する必要がなくなった。

ただしすべてのホストがクラスレス・ルーティングをサポートしているわけではない。事実、マイクロソフトの TCP/IP はまだクラス分けアドレスを使っている。ネットワークが Windows PCで設定されているときは、サブネットマスクをドットで区切った 10 進法で表記しなければならないのだ。

IP アドレスと音声ネットワーク

音声ネットワークで一般的な IP アドレスの設定を表にしてみた。

IP アドレスを割り当てると、音声ネットワークのデバイスは SNMP マネージメントプロトコルなどレベルの高いプロトコルで通信できるようになる。

デバイスの種類	IP アドレスの範囲
音声デバイス	192.168.100.1 ～ 199
スイッチングハブ	192.168.100.200 ～ 219
他のデバイス	192.168.100.220 ～ 254

表 4-2　音声ネットワークの一般的な IP アドレス

ネットワークの設計と構築

設計に入る前にスイッチングネットワークデザインのルールを振り返ってみよう。

- 利用可能なバンドワイズを超えないこと
- 距離の限界を超えないこと
- カテゴリ 5 の場合は 100m を超えるケーブルを使わない
- マルチモードファイバーの場合は 2km を超えるケーブルを使わない
- スパニングツリープロトコル 、リンクアグリゲーション、メッシュに対応したスイッチングハブを使わない限りループは作らない

さて、ネットワークを設計するときの最初のステップは適切なコンポーネントを選ぶことだ。音声ネットワークのために、最良の策は Ethernet スイッチングハブを使うことだろう。

リピーターハブよりも拡張性と柔軟性に優れ、管理機能を持たないものなら価格も手ごろだ。

次に CAT5 か光ファイバーケーブルでデバイス同士を接続する。このときデバイス間の距離がわからないとケーブルの限界距離に配慮できないため、ふさわしいケーブルを選べない。

PCに IP アドレスを割り当てる

Windows のパソコンに IP アドレスを割り当てるときはネットワークのプロパティを使う。Windows のバージョンによって正確な手順 (メニューの選び方、ウインドウの種類など) は異なる。

スイッチングハブを配置する

設定が必要なのは、通常管理機能を持つスイッチングハブを使っている場合だけだ。たいてい工場出荷時のデフォルトで十分だろうが、IP アドレスとサブネットマスクだけは割り当てなければならない。これから紹介する設定手順は Windows のパソコンでスイッチングハブを設定するときのものだ。

パソコンとスイッチングハブの COM ポートをヌルモデムケーブルで接続し、ハイパーターミナルでスイッチングハブのコンフィギュレーションメニューにアクセスする。ハイパーターミナルの安全な設定は、9600baud、8 ビット、パリティなし、1 ストップビット (8N1) だろう。

接続したら設定とコンフィギュレーションのオプションが使えるようになり、IP アドレスとサブネットマスクも割り当てられるようになる。たいていのスイッチングハブでは名前や設置場所、連絡先を登録するできるようになっているが、入力しなくてもかまわない。

接続テスト

デバイスがネットワークに接続しているかどうかをテストする最速で最も簡単な方法は、おそらく ping コマンドだろう。ping は特定の IP アドレスがアクセス可能かどうかを調査するコマンドで、ネットワーク接続のトラブルシューティングに便利なユーティリティーだ。ping コマンドを出力すると ICMP(Internet Control Message Protocol) パケットが指定されたアドレスに送られ、返答を待つ。返事が来ればそのデバイスはネットワークでアクセス可能だ。返事がなければネットワーク上の通信に問題がある。

ping コマンドを出すにはコマンドプロンプトを開けてタイプする。

```
ping xxx.xxx.xxx.xxx
```

ここで xxx.xxx.xxx.xxx は調査したいデバイスに割り当てられた IP アドレスだ。

Chapter 5　ネットワークで音声をルーティングする

はじめに

音声をデータネットワークで分配する方法は多い。使用する方法はネットワークの能力やアプリケーションの必要条件で決まる。

ネットワークにおいて最も優先されることはバンドワイズと信頼性だ。アプリケーションを考えるとき最も重要なことが音声の能力、品質、レイテンシーだ。

ファイルを転送してから再生する

ファイルを転送してから再生する音声分配法には音声サーバと再生機がいる。ファイル転送後に再生するシナリオでは、すべての操作が再生機から始まることになるだろう。再生機の指示によってサーバに保存されている音声ファイルが再生機のローカルストレージ (すなわちハードディスクドライブ) に伝送され、コピーを作成する。それから再生機がローカルでファイルのコピーを再生する。

転送には FTP(File Transfer Protocol)、HTTP(Hyper Text TransferProtocol)、NetBIOS、Napster 専有プロトコルなどのネットワークファイル転送プロトコルを使えばいい。

このスキームではファイル形式が音質を決める。一般的な WAV ファイルのような生の PCM データだと音質は最も高いだろう。MP3 のように音質を損うほど圧縮したフォーマットだと必要なバンドワイズを減らせる。

ルーティングはネットワークアドレスとファイル名で決める。

ファイル転送と再生の操作という別個の操作を 1 つのプロセスに自動化することができ、スケジュールやユーザインタフェース、コンタクトクロージャから作動できる。ファイルはそのネットワークのレートで転送される。ローカルストレージへのファイル転送が完了すると再生が始まる。

メリット

ファイルを転送してから再生する方法は常に信頼性が高い。データの完全性はファイル転送中に確認され保証される。どんなに経済的なファイル転送プロトコルでも完全性チェック機能をサポートしているのだ。これはネットワークプロトコルにもいえる。ネットワークでの配送が遅れればファイルの再生も延期されるが、ファイルはローカルストレージから再生されるため再生が始まれば中断されることはない。ネットワークリソースは再生プロセスに関係しない。

音声はネットワークの特性にかかわらず高品質だ。ネットワークのビットレートは音声のビットレートからデカップリングされる。音声のビットレートがネットワークビットレートより大きい場合は再生まで長時間待たされることになるが、要望通りのビットレートで音声を再生できる。音は良いだろう。それに何度でも再生できる。音声データがローカルストレージにあるためネットワークに戻ることなく何度でも再生できるのだ。著作権者は不利益を被ることになるだろう。

デメリット

転送後に再生するモデルが持つデメリットの 1 つは、再生する前にダウンロードを完了させなければならないということだ。待ち時間はプログラムの長さとネットワークのスピードに比例する。ネットワークが遅くて音質が良いとなれば何よりも忍耐が必要だ。

本格的なローカルストレージが必要な場合もあるだろう。プログラム全体を保存できるだけのローカルストレージが必要だ。そんなわけでたいていのアプリケーションでは再生機のハードディスクドライブにお呼びがかかる。

ファイル転送をベースにした音声ルーティングモデルはライブプログラムのストリーミングに適していない。ファイルの大きさがわからなければ転送できないのだ。

用途

ポストプロダクションのエンジニアはたいていサーバから 1 つのプロジェクトをダウンロードし、それを聞いて編集し、再びアップロードする。

MP3.COM や Napster のようなメディア配給会社はファイル転送後に再生するモデルを使っている。また家庭向けのブロードバンドを使ったオンデマンドビデオにも使われるモデルだ。設置されたトップボックスにはビデオファイルを保存するためのハードディスクが入っている。

パソコンを使った教育でも学生たちが講義や実習をダウンロードして自分のペースで学習している。

この方法は交通機関 (空港や鉄道など) で時刻通りにアナウンスを放送するためにも使えるだろう。

ネットワーク越しの再生…「引っ張る」モデル

この「引っ張る」モデルは転送後再生モデルの改良版だ。このモデルならファイルを転送し終わる前に再生を始められる。実際にデータの最初数ブロックを受信すれば再生を開始できるが、多くの再生機ではネットワークが切れたときの防護策として再生前に大量のブロックをバッファに取り込む。

この方法を「引っ張る」モデルと呼ぶのは、再生機がサーバからのデータフローを制御しているからだ。再生中にバッファに入っているデータを消費するにつれ、再生機はサーバに追加のブロックを要求する。

メリット

ファイル転送中に再生を始められる。ローカルストレージもさほど大きくなくていい。

デメリット

「引っ張る」モデルでの再生はネットワーク中断に左右される。再生が始まるとネットワークとサーバの間は音声のビットレートでデータを転送できなければならない。転送が遅れれば再生が中断される場合もある。

音質はネットワークのバンドワイズで制限される。ネットワークのバンドワイズが 56kbits/sec に制限されている場合は 128kbit/sec の MP3 ファイルを再生できないだろう。

用途

サーバの容量を共用して、MP3 を使った単純なジュークボックスを作れる。WinAmp のようなアプリケーションを使ってワークステーションで再生させればいいだろう。

サーバとネットワークが適切な特性を保てるなら、ポストプロダクションの編集者はサーバのファイルで直接作業ができるため、ローカルにコピーするための時間やストレージもいらない。こうした作業には「引っ張る」モデルがよく使われている。

ネットワーク越しの再生…「押し込む」モデル

この方法では再生機がストリーミングサーバとの接続を開いている。この接続を使ってサーバは要求された音声を再生ビットレートで送りつける。

「押し込む」モデルと呼ぶのは、サーバが再生機に向かうデータフローを制御するためだ。サーバは音声のビットレートでデータを送信する。サーバは再生機がそのビットレートで素材を再生すると想定しているのだ。再生機からサーバへの最初の要求はデータルーティングパスで決まり、音質を指定することもある。データは TCP のような「頼りになる」転送方式や、より一般的には UDP のような「頼りにならない」転送方式でサーバーから再生機まで送られる。

公共のインターネットではパケット損失はよくあることだが、こうなると再生機はサーバに失われたデータの再送信を要請することもある。頼りになる転送方式を利用していれば自動的に再転送される。頼りにならない転送方式を使うと、再転送が受信できないかあまりに遅いとき再生機が再生を見合わせるよりもミュートしたりエラーをごまかしてくれる、という利点がある。

メリット

「押し込む」モデルではバンドワイズの安定性が求められ、理想的とはいえないネットワーク環境にも順応できる。転送レートはサーバが決める。一般的にはあらかじめ音声ビットレートでバッファにデータをためるため再生までに時間がかかるが、ネットワークのスムースな特性を保証する。サーバは自身やネットワークの混雑に応じて要求されたビットレートを活動的に調整することができる。

「押し込む」モデルはライブストリーミングにも対応する。このスキームではファイル転送について説明しなくても良いだろう。サーバが再生機にデータを送っているのだ。つまりデータはファイルでも他のサーバのサウンドカードに入ってきたライブサウンドでもかまわない、というわけだ。

デメリット

この方法最大のデメリットは音響特性が冴えないことで、これは音質を損なうほど過激にデータを圧縮し、長時間バッファするためレイテンシーが高くなるからだ。しかしこうした特徴は「押し込む」モデルに固有のものではない。

公共インターネットを使った「押し込む」モデルでは圧縮とバッファリングの両方が特性に大きく影響するが、その公共インターネットではこの「押し込む」モデルが最も広く使われている。

データを圧縮すれば必要なバンドワイズが減る。公共インターネットでバンドワイズを制限している要因は 2 つだ。

1. インターネットへの接続では速度が問題になる。生の PCM でCD並みの音声は 1 チャネルで約 700kbit/sec というのが目安だ。
2. サーバの接続が高速でもたくさんの再生機にデータを提供している場合は 1 台ずつに使えるバンドワイズは限定されてしまう。

安定しないネットワーク特性に対する回復力をつけるため、レイテンシーが故意に加えられる。より多くのデータをバッファに蓄えておくことで、再生機は転送のミスや故障による遅れ、壊れて届けられたデータに対抗する。適度なバッファリングでデータ損失の際に再送信を要求する時間を稼げる。転送が遅れたり届いたデータが壊れていたり、パケットが損失するのは公共のインターネットでは当たり前だ。

同期ストリーミング

同期ストリーミングは最もシンプルなデジタル音声の転送手段だ。点と点の間で AES3、オプチカル ADAT、MADI

のようなデジタル相互接続に使われる。D/A コンバーターと A/D コンバーターは同期インタフェースを使っている。一般電話ネットワークは同期ストリーミング分配システムだ。

メリット

同期分配システムは特化されたもので、目的に合わせて作られる。目的に合わせて作られるのだからその用途に最高の解決法だろう。最も単純なソリューションは、音響機器内部で A/D コンバーターとDSPの間の短い接続や、プログラムコピーのためにCDプレーヤーと DAT を接続するような、点から点への分配だ。

デメリット

同期ストリーミングは効率的にさまざまなサービスをサポートしない。同期ストリーミングで非同期データを転送するのは能率的ではないし、破裂的なトラフィックパターンに順応しない。

変更に対応しないため、同期システムは目的に合わせて作られる傾向がある。目的に合わせて作った通信システムは費用効果が高くない。他方でより一般的なデータ転送はより大きな市場にまで発達していてそしてある規模の利益をあげている。一般的なデータ伝送はより単純だし、商品技術に含まれるものは共通の特徴だけなので経費も安い。

アイソクロナス・ストリーミング

アイソクロナスの動作は「押し込む」モデルによく似ているが、ネットワークは定量化できるだけの特性を要求される。このためレイテンシーは短くなるし音質は向上する。

ネットワークの等時性特性はサーバと再生機の接続で合意されるサービスによって数量化される。この合意にはバンドワイズ、転送遅延や遅延変動 (ジッター) といった内容を指定する。

「押し込む」モデルではサーバがデータレートを制御していたが、再生機に対して必ずしもクロックを送っていたわけではない。一般的にサーバーと再生機が両方ともジャムシンクで動いていて、各自のローカルクロックをリファレンスにしていた。クロックのわずかなレートの差はデータを分断してしまうことで処理されていたのだ。アイソクロナス・ストリーミングは同期転送にならっていて、サーバと再生機の間に共通のクロックがある。

アイソクロナス転送の送信機と受信機

データは A/D コンバーターなど同期入力に到着するとパケットに分割される。それからパケットのタイムスタンプが調べられ、転送待ちの行列に入れられる。受信機ではパケットが転送されてくると順番に並べられる。パケットのタイムス

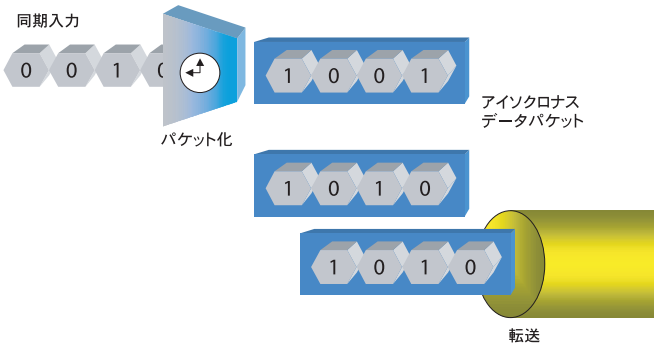


図 5-1　アイソクロナス転送の送信機

タンプを調べていつどのパケットを列から出すかを決めるのだ。これがバッファを持つ受信機のスキームで、壊れたデータパケットの受信を延期するなど故障にも対処できる。

送信機と受信機は同期インタフェース用のクロックを持っている。クロックはいくつかの方法で同期されていなければならない。クロックを同期するときのスキームには下記の例がある。

- 別のケーブルや GPS 受信機などを使って帯域の外でクロックを分配する
- 受信機のクロックがデータを受信したタイミングや完全な列の受信を基準にする
- 特殊なデータパケット用の帯域を使ってクロック情報を運ぶ

受信機のクロックは送信機のクロックに対してオフセットして動いている。このオフセットはデータをパケット化して転送する時間を稼ぐためだ。可能な最小オフセットは 1 パケットのデータを作って転送するために要する時間だ。

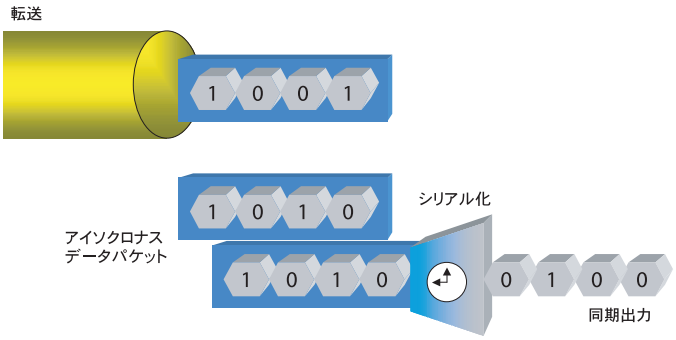


図 5-2　アイソクロナス転送の受信機

メリット

アイソクロナス転送の合意でネットワークの特性が安定しているため、レイテンシーが短くなる。

品質も高い。アイソクロナス・サービスの合意は広いバンドワイズを指定しているため、明瞭度が高く圧縮していない音声に対応する。

ストリーミング能力も備わっている。同期からアイソクロナスへ、あるいはアイソクロナスから同期へと変換するときに必要なクロックの分配が本来のデジタル音声ストリーミングに提供される。アイソクロナス・ストリーミングは非同期の接続をエミュレートしている。

デメリット

デメリットの 1 つはデータネットワーク上で広く利用できるものではないことだ。これは QoS の合意と密接に関係している。QoS はまだデータネットワークに参入してきたばかりだ。基礎をなしているネットワークからのサービス合意に加えて、データ転送のためのフレームワークが必要とされる。CobraNet は Ethernet にこのフレームワークを提供する。ATMや IEEE1394 のような他のネットワーク技術のために、アイソクロナス転送は不可欠なサービスだ。

もう 1 つのデメリットはしばしば点から点への接続に限定されるということだ。たとえばアイソクロナス・サービスはよく同期転送を使っている。この例が ISDN 接続の電話会議だ。ISDN は各方向に 64kbits/s のスループットを保証している。アイソクロナス・サービスを提供する基礎にふさわしい単純な QoS 協定だ。

CobraNet

CobraNet はハードウェア (CobraNet インタフェース) とネットワークプロトコル、ファームウェアを組み合わせたものだ。CobraNet はスイッチング Ethernet ネットワークや専用の Ethernet リピーターネットワークで機能する。CobraNet は Ethernet ネットワーク上で下記の追加通信サービスを提供する。

- アイソクロナス転送
- サンプルクロックの分配
- 制御と監視データの転送

CobraNet インタフェースは同期からアイソクロナスへ、アイソクロナスから同期への変換はもちろん、リアルタイムにデジタル音声をネットワークで伝送するために必要なデータフォーマット化も行う。

CobraNet インタフェースは SNMP(Simple Network Management Protocol) のような制御や監視のデータを、音声と同じネットワーク接続で伝送したり利用する準備もしている。CobraNet は Ethernet ベースなので、Ethernet のデータ伝送性能はコンピューターのデータとして表示されることになる。ほとんどの場合、データ通信と CobraNet アプリケーションは同じネットワーク上で共存できる。

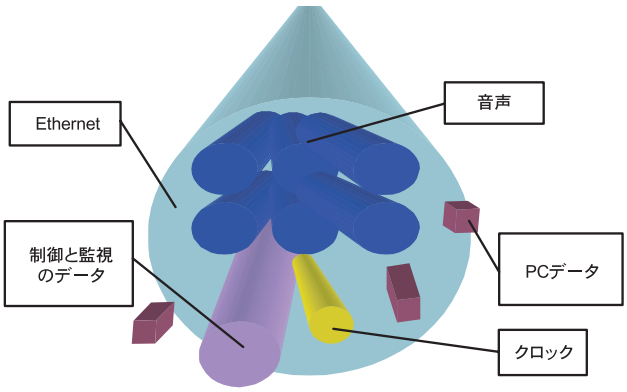


図 5-3　CobraNet のデータサービス

CobraNet 用語

CobraNet は音声とデータ通信という2つの業界にまたがる技術だ。各業界にはそれぞれ不可解な専門用語が存在するが、下記は CobraNet そのものに関連したものだ。

CobraNet インタフェース…CobraNet インターフェースはハードウェア (あるいはハードウェアの設計) と Peak Audio が CobraNet ライセンス所有者と関係団体に提供するソフトウェアから成る。

CobraNet デバイス…CobraNet インタフェースを搭載した機器を指す。

コンダクタ…コンダクタ (指揮者) はネットワークにマスタークロックを供給し送信を裁定するために選ばれる CobraNet インタフェースを指す。コンダクタの役割と選ぶ方法は後述しよう。ネットワーク上の他の CobraNet デバイスはすべてパフォーマ (演奏者) の役割を果たしている。

音声チャンネル…プロオーディオの業界では音声チャンネルの意味は完全に明確であるべきだ。CobraNet ではサンプリング周波数 48kHz、分解能は 16、20、24 ビットのいずれかを選択できるデジタル音声を指す。

バンドル…バンドルは最も小さいネットワーク音声のルーティングエンベロープだ。バンドルはアイソクロナスサイクルごとの Ethernet パケット 1 つを表している。バンド

ルは 0 から 8 つの音声チャネルを運べる。また 1 から 65279 までの番号が振られている。バンドルは 1 つの送信機を持っている。バンドルには 2 種類ある。

マルチキャストバンドル…バンドルナンバー 1 から 255 まではマルチキャストバンドルだ。このバンドルは受信されているかどうかにかかわらず常に音声を伝送する。1 対多の接続が可能だ。マルチキャストバンドルに関連するデータパケットにはマルチキャストアドレスがつく。

ユニキャストバンドル…バンドルナンバー 256 から 65279 までがユニキャストバンドルだ。1 対 1 の接続だけが許される。データを流す前に送信機と受信機がユニキャストバンドルでダイヤルイン接続されることになる。

CobraNet インタフェース

CobraNet インタフェースは集積回路だと考えられる。この集積回路のピンアサインは搭載された機器の他の部分へのインタフェースを定義する。CobraNet インタフェースの「ピンアサイン」には次の機能的なグループが含まれる。

- 音声 I/O と D/A コンバーターや A/D コンバーター、DSP との同期接続
- ホストのデジタル音声回路を同期するためのクロック I/O
- マネージメント変数 (バンドルアサインなど) と制御データ I/O のためにホストプロセッサとの接続に使うホストインタフェース
- シリアルブリッジング機能のための非同期
- バディリンク…CobraNet デバイスをバックアップ用ペアとして機能させる相互接続スキームで、メインのユニットが適切に働いている限りバックアップユニットの送信と受信を抑制する機能

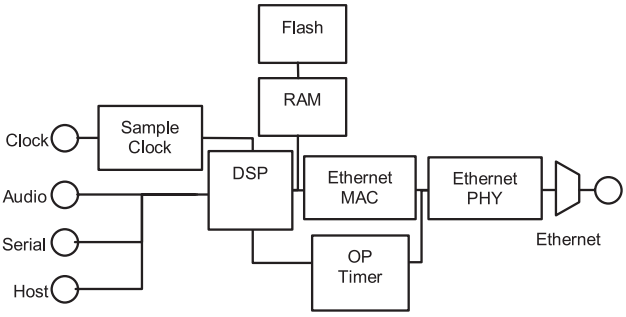


図 5-4　CobraNet インターフェース

アイソクロナス・サイクル

CobraNet はネットワークの音声トラフィックにアイソクロナス・サイクルを持ち込み、Ethernet でアイソクロナス・サービスを可能にしている。このバリエーションが IEEE1394 と USB のアイソクロナス・サービスに使われている。

アイソクロナス・サイクルはコンダクタがビートパケットを送信したとことで始まる。音声を送信したがっている CobraNet デバイスは音声データを送信する前にビートパケットの受信を待つのだ。すべての音声データが送信されると種類の違うデータパケット、制御や監視データ、リザベーション要求などを送信できる。

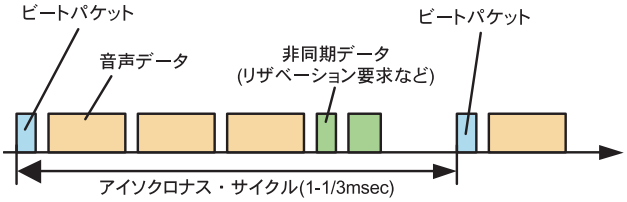


図 5-5　アイソクロナス・サイクル

コンダクタ

コンダクタはネットワークにマスタークロックを供給する。クロックはビートパケットの送信タイムスタンプで分配される。パフォーマは受信したビートパケットに同期するようローカルクロックを調節する。ローカルクロックは安定性の高い電圧制御水晶発振器 (VCXO) で生成される。音声に影響を与えるジッターなどの副産物を避けるため、ローカルクロックの調整はスムーズな方法で行われる。

コンダクタはバンドワイズとネットワークのルーティングリソースを裁定する。CobraNet デバイスがネットワークに送信したい場合はコンダクタに予約を申し入れる。コンダクタはこの申し入れを承認するとビートパケットに許可項目を加える。ネットワークのバンドワイズが不十分だったり、要求したバンドルが他の送信機に使われている場合、コンダクタはリクエストを拒否できる。

コンダクタの調停

コンダクタは調停手続きを経て選出されるが、そのデバイスはプライオリティの最も高い優先権を宣言したことになる。コンダクタと同じプライオリティを持つ CobraNet デバイスがネットワークに入ってくると、不意にコンダクタが交代しないよう防止策がとられる。コンダクタが突然オフラインになったとき、同程度の優先権を持つデバイスが複数あると次のコンダクタの座を競い合うことになるが、この場合は Ethernet の MAC アドレスがタイブレーカーになる。

CobraNet デバイスはすべて、ネットワークでコンダクタの役割を担うために必要なリソースを搭載してる。コンダクタが切り替わるときネットワーク上で一瞬だけ (10ms) 音声が止まる。コンダクタの優先権は多くの CobraNet 製品でユーザ設定可能になっている。CobraNet の大きなシステムを設計するとき、コンダクタとしての優先権が高い機器を UPS(無停電電源) に接続し、中央で制御したいと考えることも多いだろう。デジタル同期の問題がいくつか、同じくコンダクタの優先権を使って扱われる。

CobraNetプロトコル

CobraNetプロトコルはデータリンク層 (OSI レベル 2) で機能する。CobraNet には基本になるパケットタイプが3つある。すべてのパケットは Peak Audio 割り当てられた独自のプロトコル識別子 (0x8819) で識別される。

ビートパケット

ビートパケットにはマルチキャストアドレスが割り当てられているので、ネットワーク上すべてのデバイスが受け取る。到着時間とタイムスタンプによってビートパケットはネットワーク上すべての CobraNet デバイスにサンプルクロックを配る。ビートパケットにある許可リストにはネットワーク上への送信を許可するデバイスが表示されている。リピーターネットワークの場合は、コリジョンを避けるようにビートパケットで送信順を決める。

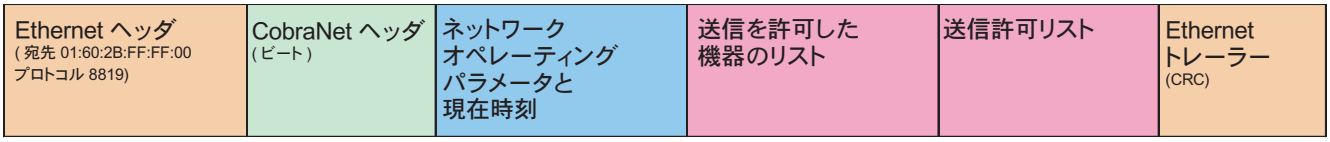


図 5-6　ビートパケット

リザベーションパケット

リザベーションパケットはおよそ 1 秒間隔ですべての CobraNet デバイスから送信される。コンダクタはネットワークの特性報告に基づいてリソースが利用可能かどうか、いつ新しい音声の送信要求に答えるかを定義する。予約を申し入れるとき IP アドレスを明確にするため、CobraNet デバイスのリストとその IP アドレスが Disco や CobraCAD のようなユーティリティでも利用できる。

フォワードリザベーションはコンダクタに申し入れられる送信要求で、コンダクタは送信許可を求められる。リバースリザベーションは受信要求でデバイスが受信したがっているバンドルを列挙したものだ。リバースリザベーションは要求されたバンドルの送信機になりうるデバイスに向けられる。リザベーションパケットにはマルチキャストアドレスが付く。これには 2 つの理由がある。まずコンダクタだけではなくコンダクタになりうるデバイスすべてにリクエストの内容を知らせるためだ。これならコンダクタに異常があってもスムーズに交代できる。また全送信機はリバースリザベーションをすべて調べ、それに反応して送信を開始すべきかどうかを判断するのだ。

図 5-7　リザベーションパケット

音声データパケット

音声データパケットにはデジタル音声データが入っている。データは 16、20、24 ビットのいずれかだ。すべて圧縮されていない PCM データだ。

音声パケットは伝送に使うバンドルによって、マルチキャストとユニキャストのどちらかになる。

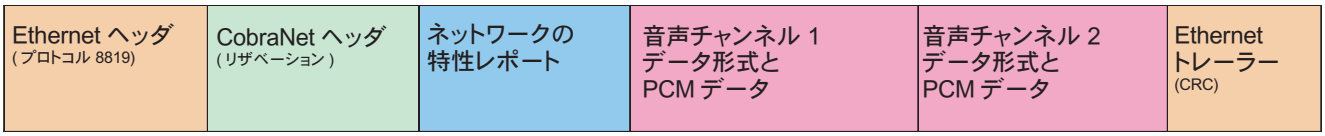


図 5-8　音声データパケット

Chapter 6　ネットワークの管理と制御

はじめに

音声ネットワークを使うことの重要な利点は、中央からネットワークに接続した全デバイスを制御したり監視できることだ。この章では SNMP を使った制御と監視、さらにネットワーク管理の基本を紹介する。

ネットワーク管理とは？

ネットワーク管理とは、ネットワークの状態と効率を維持するためのプロセスを集めたものだ。監視も含まれる。

・セキュリティー…無許可のアクセスから保護
・特性…ボトルネックを排除する
・信頼性…ネットワークを確実に利用可能な状態にする

ネットワークの管理はネットワークの大きさとは関係がない。何百、何千というパソコンや周辺機器を接続したネットワークを管理する場合の技法を、わずか数台の CobraNet デバイスからなる音声ネットワークに使えるのだ。

管理されたネットワーク上にあるデバイスは 3 つのカテゴリーに分けられる。

1. 管理ノード…クライアント、マスター、マネージャーなどと呼ばれることがある
2. 管理されたノード…サーバ、スレーブなどと呼ばれることがある
3. 管理されていないノード

管理ノードは一般的にワークステーションやネットワーク管理アプリケーションを起動するパソコンを指す。その唯一の目的は管理されたノードから情報を収集することだ。管理されたノードはマネージャーからの情報要求に応じる。マネージャーが管理されたノードへのアクセスを許可されている場合、管理されたノードは要求された情報を集めてマネージャーに返信する。管理されたノードの例はパソコン、Ethernet ハードウェア、CobraNet デバイスだ。

管理されていないノードは互換性のない管理プロトコルをサポートしているか、あるいはまったく管理機能を持っていないのだろう。こうしたデバイス用のプロクシがあって管理機能されていないノードが「会話」できる場合もある。

管理と制御のプロトコルにはさまざまなものがある。中には指定されたデバイスでだけ作動する専用のものもある。アンプの制御スキームがたいていこのようにして作用する。他のプロトコルは特定のパソコンに機能するものなので、特定したパソコンに関する情報がメーカーから提供されている。パソコンを特定したプロトコルの中にはネットワーク規模の管理プロトコルへのインタフェースを持つものがある。この章ではネットワーク上のデバイスを制御するための基本的なツールの他、SNMP と呼ばれるネットワーク規模の管理プロトコルに焦点を合わせる。

Telnet、HTTP、FTP

前の章で紹介した通り、管理機能を持つ Ethernet スイッチングハブはハイパーターミナルを使ってコンソールセッションで構成を設定できる。この種のセッションが最も使われるのはスイッチングハブに IP アドレスを割り当てるときだ。コンソールセッションはパソコンと管理されたデバイスを直接ケーブルで接続しなければならないので、広いエリアに散らばる多くのデバイスからなるネットワークを長期的に管理するにはそれほど便利ではない。しかし IP アドレスが割り当てられれば、Ethernet スイッチングハブだけではなく他の管理されたデバイスにも離れた場所からネットワーク経由でアクセスできるオプションもある。

Telnet

Telnet は TCP/IP ネットワークで使われる端末通信プロトコルだ。ローカルのパソコンで動作しネットワーク上のリモートサーバに接続可能にするものだ。この場合、サーバーは別のパソコン、スイッチングハブなど Telnet サーバを作動できるデバイスだ。Telnet セッションを通してローカルのパソコンに任意のコマンドを入力すれば、そのリモートデバイスに直接入力したかのように実行される。

コンソールセッションと Telnet が管理機能を持つスイッチングハブの構成を設定するとき最も包括的なアクセスを提供する。コンソールセッションとは異なり、Telnet セッションはリモートデバイスにアクセスするときユーザ名とパスワードを要求する。しかしこのアクセス制御はアプリケーション層のものであり、コンソールセッションにしても Telnet にしても不安定だ。

HTTP

管理されたデバイスの中にはウェブブラウザや HTTP インタフェースで構成を設定できるものがある。Telnet 同様そのデバイスは TCP/IP ネットワークにアクセスできなければならない。つまり IP アドレスを割り当てなければならないのだ。

ただウェブブラウザを起動して管理機能を持つスイッチングハブの IP アドレスをタイプすれば、インターネットでウェ

ブページを見るかのように構成を設定できる。実際に情報は管理されたデバイス自身の中にあるウェブサーバが提供している。

管理機能を持つスイッチングハブには HTTP アクセスを一部の機能設定にだけに制限しているものがある。ウェブアクセス可能なパラメータと同様、全体のレイアウトやウェブページ自身のナビゲーション構造はメーカーによって異なる。たいていのスイッチングハブメーカーは、カラフルなグラフやチャートでネットワークの状態を定期的に更新して表示する HTTP インターフェースを提供している。こうしたウェブブラウザ・インタフェースはネットワークの特性を管理するためには優れたツールで、スイッチングハブの状態やエラーはもちろん、スイッチングハブを出入りするトラフィックの流れなどの情報が、使いやすい簡単なインタフェースで提供される。

直接 HTTP でデバイスを管理するこの方法は、大きなネットワークを管理するには不十分だろう。

TFTP

Trivial File Transfer Protocol、略して TFTP は離れた場所にあるパソコンやデバイスでファイルを送信あるいは受信できるようにするプロトコルだ。音声ネットワークで、もっと限定すれば CobraNet ネットワークでは、ネットワーク上の音声デバイスやスイッチングハブのファームウェアをアップグレードするために使っている。

SNMP を使った管理

SNMP は Simple Network Management Protocol の略だ。管理された TCP/IP ネットワークの標準で、今日最も広く使われている管理プロトコルだ。数多い利点の 1 つは実行に必要なコードが極めて少ないことだ。つまりシステムリソースをさほど消費することなく、そしてそのデバイスの主要な機能を妨げることなく、デバイスを追加できることになる。SNMP の拡張性で既存の製品に管理能力を持たせることも簡単だ。SNMP は管理構造とハードウェア構造を分離するため、さまざまなメーカーの製品に適用できる。

SNMP の通信は無接続で「頼りにならない」User Datagram Protocol(UDP) で伝送する。つまり TCP/IP とは異なり、エラーなくパケットが転送される保証はされない。信頼性については SNMP 管理アプリケーションが担っていて、送信するメッセージをすべて記録・追跡し、メッセージが損失すれば再び送信している。

SNMP はアプリケーション層にいるソフトウェアで実行されるので、OSI 参照モデルの第 7 層で動作する。データをネットワーク越しに転送できる形式に当てはめるにはプレゼンテーション層が必要だ。

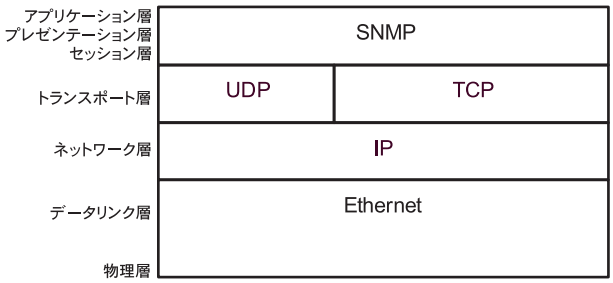


図 6-1　SNMP と OSI 参照モデル

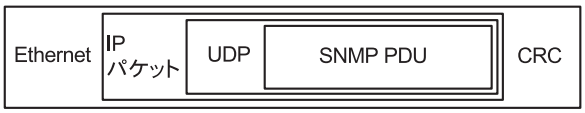


図 6-2　SNMP メッセージを運ぶ Ethernet パケット

Ethernet 上で SNMP データを運ぶには PDU(Protocol Data Units) が使われる。ある OSI の層から別の層へのデータを通過させるブロックだ。各層は独自の PDU を持っていて情報を他の層へ通過させるので、データは渡り歩くことになる各レイヤー向けの PDU にパックされていなければならない。Ethernet で SNMP メッセージを送ることは、すでに TCP/IP データを Ethernet で伝送することを説明したとき例に挙げたメールの例に似ている。

エージェントマネージャーと MIB

エージェント

SNMP エージェントは管理されたノードへのインタフェースだ。それ自身管理されたノードにあって、データを記憶したり返すことに責任をもっている。

そして望まれないトラップと呼ばれるイベントを出すという任務がある。トラップは、故障やあらかじめ定義されたスレッショルド (名前をつけられた例はほとんどない) 超過を、マネージャーから催促されなくてもすぐ管理されたノードに送る機能だ。

SNMP エージェントはまた管理機能を持たないノードの代理人としても機能する。代理人として、エージェントはマネージャーが求める管理操作を管理機能を持たないノードのために行う。この代理人はある種の翻訳者だと考えられるだろう。受け取った SNMP コマンドを管理機能を持たないノードが理解できる言語に翻訳し、そしてコマンドを出す。この逆も真で、この代理人は SNMP データをマネージャーに戻すことができる。

変数は管理されたデバイスの MIB で定義され、デバイスごとに特殊なものになる。管理されたオブジェクトとして記述されることもあり、MIB ツリーの「葉」になっている (次項参照)。MIB 変数はデバイスのハードウェアに関する情報、設定パラメータの他、特性の統計値さえ含む。管理されたデバイスの定義された MIB という情報は SNMP エージェントだけが検索できる。

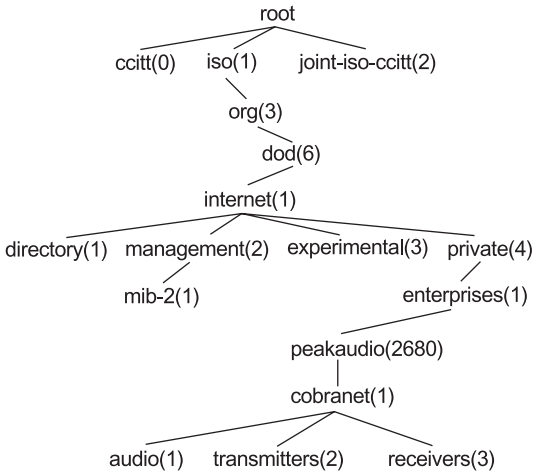
MIB

MIB は Management Information Base の略だ。マネージャーとエージェントが管理されたデバイスのハードウェアとソフトウェアに関する情報を交換するための定義だ。MIB は標準化されたフォーマットで、どんな SNMP ツールにでも MIB で定義された任意のデバイス監視を許可する。

MIB でのオブジェクトは管理されたオブジェクトのプロパティのために構造と形式が指定される。この様子は階層形式のツリー構造で表示され、それぞれの枝には独自の名前と OID(オブジェクト識別子) がついている。中間の枝は MIB に関連したオブジェクトのグループで、葉は実際には個々に識別される MIB 変数だ。MIB オブジェクトを表す完全な OID は木のいちばん上からその MIB オブジェクトを含む葉までの完全なパスになっている。それぞれの枝を区別しているのはピリオドだ。

たとえば、下図の MIB ツリーで mib-2 の枝を表す OID は、1.3.6.1.2.1　になる。

OIDs は Internet Assigned Numbers Authority によって割り当てられ、重複はしない。OID を受け取るとメーカーは必要なだけ MIB を制限なく拡張できる。



マネージャー

マネージャーは管理機能を行なうコンソールやコンピューターを指す。SNMP 管理アプリケーションを起動して SNMP エージェントに問い合わせ、エージェントから応答と共に認証イベントも受け取る 。マネージャーは SNMP をセットにすることである量の制御をこなすことができる。処理能力とデータストレージの大部分はマネージャーにあり、管理されたノードの負担を減らす。

SNMP メッセージ

SNMP エージェントの管理されたオブジェクトを操作するために、4 つの SNMP 操作がある。

1. GetRequest
2. SetRequest
3. GetNextRequest
4. トラップ

それぞれ SNMP 管理システムやエージェントが特定の情報で埋めてそれぞれの方法で送信するテンプレートのようなものだ。

GetRequest メッセージはエージェントが保守する管理されたオブジェクトから値を検索するために使われる。たとえば送信用のバンドルナンバーに関する情報を問い合わせるために CobraNet デバイスに送信されることもある。

SetRequest は管理されたオブジェクトのために値を設定するときに使われる。CobraNet デバイスのバンドルナンバー数を変えるためにもこの「Set」が使えるだろう。SetRequest はマネージャーが管理データを改造できる唯一のメカニズムだ。

GetNextRequest は GetRequest と同じだが、テーブルを横切って「歩く」ために使われる。

GetResponse は反応を返すメッセージで、エージェントが要求に応えるときに使う。CobraNet デバイスは送信するバンドルナンバーに関する問い合わせに答えるとき使う。もちろん要求がなければ反応は出力されない。

トラップと呼ばれる最後の動作は要求されないのにエージェントが送信する、誰からも望まれない反応だ。トラップはただのイベント報告で意外な状況が発生したことを示すものだ。トラップの有用性を例で示そう。音声システムのコンポーネントに異常が発生した場合、気づいたときはたいてい遅すぎている。使おうと思って電源を入れたが働かない! という経験がおありだろう。管理された音声ネットワークを使っていれば、この機能が使用前に自動的にデバイスの異常を信号で知らせるので、本番が始まる以前に対処できる。

CobraNet のエージェントはトラップをサポートしていないが管理アプリケーションの中に特定の MIB 変数を監視できるものがあるため、前もって決めたスレッショルドを超えればトラップを出力する。管理アプリケーションの MIB 変数監視能力はどんな管理されたデバイスにでも適用できる。

SNMP メッセージはそれぞれ 3 つの主要なコンポーネントから成り立つ。

1. バージョン番号
2. コミュニティー名
3. SNMP PDU

バージョン番号は使用中の SNMP プロトコルのバージョンを表す。コミュニティー名は情報を受け取るホストの管理コミュニティ名だ。一般的にはノードのグループを機能や場所、サービスしているユーザーなどの共通項を示すように付けられる。

PDU には管理されたオブジェクトの MIB オブジェクトが入っていて、実際にそのオブジェクトで実行される。多数の MIB OID と SNMP オペレーションを一つの PDU に入れることができる。

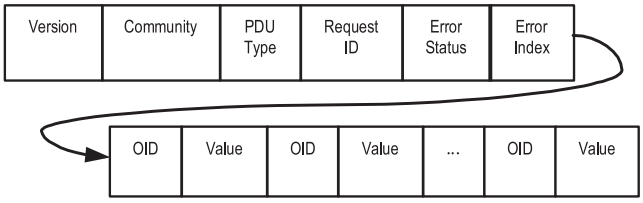


図 6-3　SNMP メッセージ

管理ソフトウェア

今日ではさまざまな管理ソフトウェアアプリケーションを使うことができ、そしてたいていの Ethernet デバイスメーカーが独自のアプリケーションを提供している。管理機能を持つスイッチングハブを買えば無料で付いてくるソフトもあるし、

「エンタープライズ」の管理アプリケーションを別に買わなければならないこともある。エンタープライズ版はより機能豊富で、ネットワークデバイスの監視だけではなくソフトウェアの制御能力を拡張するカスタムスクリプト用のインタフェースも提供するという強力さだ。

ポーリングとネットワークトポロジー

最も基本的なネットワークデバイスの状況を確認する方法は単純な ping コマンドを出力することだ。ping に反応すればそのデバイスは「目を覚まして」いてネットワーク上で通信していると考えられる。そのデバイスの状況についてさらなる情報を得るには特定の MIB 変数を問い合わせる。

エンタープライズ版はネットワークの各部分がどのように相互接続しているかをかなり詳細に表示してくれる。デバイスの状態は色で表示されていて、通常は、潜在的に問題があれば赤の、正常に動作していれば緑のアイコンが表示される。おかげでネットワークの欠陥を素早く視覚的にとらえることができる。

部分表示

ネットワークが大きくなると、一画面でネットワーク全体を表示しにくくなることがある。こうなるとたいてい、それぞれ多くのデバイスをまとめた固まりが表示される。階層が写実的に維持され、低いレベルに赤い「問題部分」があればいちばん上のレベルまですべてにその反応が現れる。

イベントログと特性

管理プログラムのほとんどにはアプリケーションがバンドルされていて、イベントを記録する能力を提供する。イベントとはトラップの送信、ネットワークの部分的なダウン、ノードの異常やサービス停止、スレッショルド超過などだ。イベントは分類されることもあり、問題箇所やその重大さを視覚的に表示してくれる。

カスタムスクリプトで SNMP トラップの利点を拡張することができる。たとえば、「デバイスがダウンした」というトラップを受け取ったら自動的に電子メールを送信するように設定しておけるのだ。潜在的な欠陥ばかりか問題のあるデバイスの名前まで自動的にメンテナンス担当者に通知してくれるのだから、トラブルシュートはより効率的になる。管理された音声ネットワークの場合、メンテナンス担当者は現場に行く前にどこで問題が発生しているか知っていることになるのだ。

より強力なエンタープライズ版にはチャート表示機能があり、バンドワイズの使用状況などネットワークの傾向を教えてくれる。また特定の MIB 変数などユーザーが指定した基準に合わせてカスタマイズしたチャートを表示してくれる。

Chapter 7　特殊なニーズに合わせて設計されたネットワーク

高可用性

システムは多くの次元で高可用性を実現できる。システムの有効性を測る手段には次の項目がある。

・稼働率
・平均故障間隔
・修復にかかる平均時間

高可用性デザイン

どんなシステムでも高品質のコンポーネントを指定したり、ホットスワップ対応のコンポーネントを使ってバックアップコンポーネントを加えれば可用性を改善できる。

高可用性システムは、決して故障を許されない、仮に故障しても素早く復旧しなければならないシステムに分類される。この2つの必要条件には異なるアプローチが必要だろう。

これから紹介する手法はシステムの有効性を向上するために使えるだろう。設備に合わせてこれらのテクニックをミックスして調和させ、バランスを取るといい。

質が高いコンポーネント

システムのレベルは最も弱いリンクで決まる、と言うと誇張かもしれない。だがシステム中に信頼性の低いコンポーネントがあればシステム全体の信頼性に影響を与えることは確かだ。質が高いコンポーネントを選択するとき問題になるのは、マーケティング戦略が生んだ戯言を乗り越えて質が高い物を探すことだ。ここでは簡単にアドバイスできない。

Ethernet や CobraNet のような既製の技術を使う場合、質の高いコンポーネントはかなり入手しやすい。

コールドスペア

予備の部品を身近に持っているだけでも可用性を改善できる。メンテナンス担当者のトレーニングにも予備コンポーネントは有用だ。ただし仕様通りに設定しておき、スタッフのトレーニングを視野に入れていただきたい。

ホットスワップ

システムの他の部分を通常 (あるいは能力がやや低下した状態で) 稼働させておきながら故障した部分を交換できれば可用性は上がる。

Ethernet 接続はすべてホットスワップ対応だ。ネットワークデバイス (特に大きいコアスイッチ) によっては電源部やインターフェースカードなどがホットスワップに対応している。

故障時の切り替え

バックアップコンポーネントをホットスペアとして待機させておくこともできる。ホットスペアは故障が発生すると自動的にあるいは手作業で登板させられる。修復にかかる平均時間を短縮できる効果的なアプローチだ。ただし故障の定義によっては、故障時の切り替えというソリューションがシステムの平均故障間隔に影響する場合もしない場合もあるだろう。

障害に対する強さ

バックアップコンポーネントを接続してシステムの負荷を分担しながら連続動作させることができる。音声のシステムでいえば、必要以上の音量を提供できるだけのスピーカーを持ち込み、1つや2つのチャンネルが機能しなくてもシステム全体として十分機能するように考えるのと同じことだ。

このアプローチ最大の利点はシステムのあらゆる部分が動作し続けるということだ。数週間も前にバックアップユニットが無言のうちに壊れていた、などということもなくなるだろうし、セーフティネットなしで運用することはなくなるだろう。

環境の要因

可用性は外部要因によっても低下する。たとえばサージプロテクションや接地、アイソレート、避雷針システムには特別な注意を払うべきだろう。光ファイバーは EMI に強いし雷からのアイソレートもできている。CAT5 の 100BASE-TX Ethernet インタフェースには 1000 Vアイソレートトランスが搭載されている。電源の信頼性も算定しておき、必要であれば無停電電源装置 (UPS) を使用すべきだ。パソコンのように再起動に時間がかかるコンポーネントに UPS を使用すれば、修復にかかる平均時間を短縮できる。

監視

異常発生後、警告のためただちに赤いライトが点灯したり自動的に発信されれば、修復にかかる平均時間は短縮される。早く警告されればより早く問題を解決できることは明らかだ。故障する前 (たとえばファンが故障したがまだ煙は出ていないとか、ハードディスクの修復回路がマージナルデータを検出したといったとき) に警告を受け取れればなお良い。音声の世界でははるかに遠い取ってつけたような概念に見えるかもしれないが、データ通信の世界では日常的に行われていることだ。

従来のアナログ音声システムは実際に使ってみるまで多く

の故障は検出されない。これはシステムの音声分配が一方向だからだ。アンプが出力した音声はアナログケーブルを通ってスピーカーに行くが、音声が目的地に到達したことを知らせるリターンパスはない。

ネットワークは双方向性 (さらに多方向) に通信メディアを提供する。プログラムがない場合でさえ承認が継続するので、通信や音声のリンクにどんな異常があっても通知される。

双方向性システムでの「承認」がより早く問題を識別して修正するのに役立つ。「スピーカー W23 番の高域ドライバーでインピーダンスの悪化を検知」すると「向こうの端あたりでは少しくすんだ音がするようになった」と対照できるのだ。

生命の安全

警報システムの可用性については違った定義が必要だ。こうしたシステムは異常な (建物が燃えているなどの) 状況の下で稼働し続けることを期待されているからだ。

警報システムにはよく監視コンポーネントが必要とされる。こうしたシステムはごくたまに使われるものだが、お呼びがかかったときにシステムが稼働するだろうことを知る手段は不可欠だ。ネットワークで接続された音声分配システムの双方向通信ならその要望に応えられる。

ネットワークの可用性

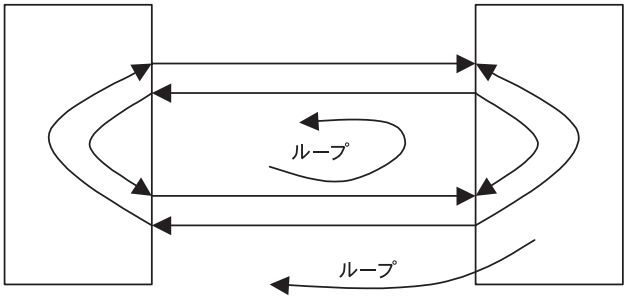
Ethernet は世界中で重要なミッションに使われている。Ethernet ベースのネットワークで高可用性を達成するためには既製の、そして標準化された多くのテクニックがある。これは音声分配に広く使われている技術を適用したことの大きな利点だ。Ethernet の可用性を向上する技術を紹介しよう。

リンクアグリゲーション (トランキング)

どんなネットワークでも Ethernet スイッチングハブを2つや3つ相互接続することになるだろう。スイッチングハブ間のリンク1つで多くの音声チャネルを運ぶことになるかもしれない。バンドワイズを考えるとそのリンクに大きな負担がかかっていることもあり得る。そのリンクがなくなれば可用性にも問題が出るだろうし、システムの機能上受け入れ難い部分がダウンすることも考えられる。

リンクアグリゲーションは両方の問題を解決する。これはスイッチングハブの間に複数のリンクを平行させておき 1 つのリンクとして機能させる方法だ。ふつうスイッチングハブの間を複数のリンクで並列に接続するとループができる。しかしリンクアグリゲーションはループを阻止してくれるのだ。接続はすべてアクティブなまま、トラフィックは両方のリンクをバランスよく渡っていく。これでスイッチングハブ間のバンドワイズが増える。またリンクがどれか故障すれば残った

リンクアグリゲーションがない場合 - ループが発生



リンクアグリゲーションの場合 - ループは発生しない

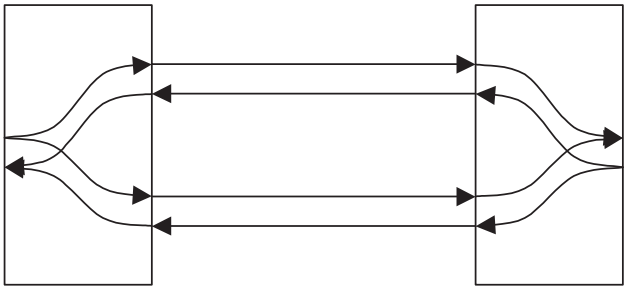


図 7-1

リンクアグリゲーションは複数 (この例では 2 つ) のリンクを使って高容量のリンクを 1 つ作る。スイッチングハブ同士を平行に接続したとき通常は発生するループは排除される。

リンクがすぐに引き継ぐ。すべてのリンクが常にアクティブなので、故障時の引き継ぎによる遅延は基本的に発生しないのだ。

リンクアグリゲーションに関する IEEE の規格 (802.3ad) は最近できたばかりだ。規格化される前にメーカー各社が独自のスキームを発表したので、業界全体で相互作用するものはまだない。3Com のものはポートトランキングと呼ばれている。Cisco 専用のものは Fast EtherChannel という名前だ。

リンクアグリゲーションを使うためには、スイッチングハブを適切に設定する必要がある。手作業でポートをアグリゲーショングループのメンバーに指名しなければならないのだ。

スパニングツリープロトコル

スパニングツリープロトコル (STP) は Ethernet ネットワークでループを阻止するために設計された。ループはそれだけで可用性に問題を起こすことがある。人的ミスやサボタージュ、破壊行為といった故障の原因になり得る事柄と同じで軽視できないだろう。ところがループ問題を解決するためのスパニングツリープロトコルは意図的にループを作れるようにする。ループがバックアップパスになり、環状トポロジーが異常に強いシステムを作るのだ。

スパニングツリープロトコルは打診用のパケットを送り、ネットワークの配線方法を決めて機能する。スイッチングハブ自身がこうしたパケットを生成するのだ。スパニングツリープロトコルはまずポートを使えない状態にしておき、アルゴリズムでネットワークにループを作らない接続を定義し、それから接続を使えるように戻す。スパニングツリープロトコルのアルゴリズムによって作られた、あるいは無効にされた接続でネットワークを再評価する。このようにして万が一のときはリンクの異常やスイッチングハブの故障さえ迂回するよう、使用不可能にしたリンクを使って経路を決めるのだ。

スパニングツリープロトコルはずいぶん前からある IEEE 規格 (802.1D) だ。15 年のサービスで広く使える一般的な解決策になった。スイッチングハブで一般的に使用できるほどシンプルなものになった。Cisco のスイッチングハブならほとんど工場出荷時のデフォルトで使用可能になっている。

このプロトコルは安全だが遅いアルゴリズムだ。どんなリンクでも可能だが瞬間的にさえループになることはない。ただしネットワークに異常が発生してこのプロトコルが新しい接続を使えるようにしたり、既存の接続を有効や無効に切り替えるためには 30 秒ほどかかる。

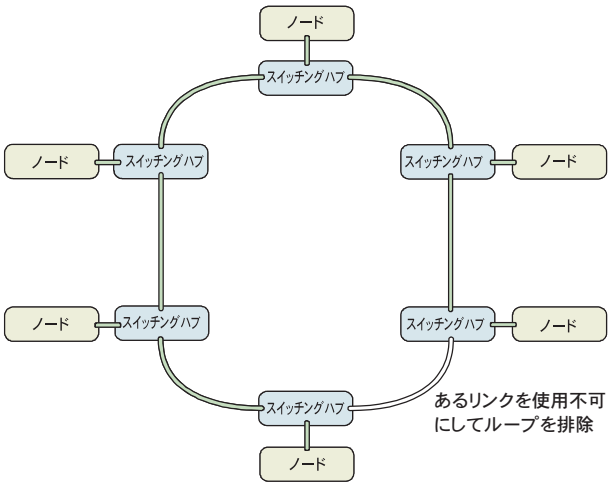


図 7-2 スパニングツリープロトコルが使用不可にしたリンク

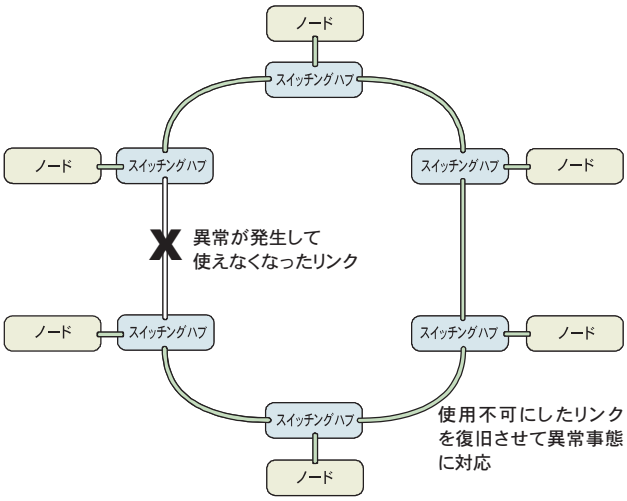


図 7-2 スパニングツリープロトコルが再使用可能にしたリンク

メッシュ

メッシュはHPのスイッチングハブ ProCurve ファミリーでだけ利用可能だ。この特徴はスパニングツリープロトコルとリンクアグリゲーションを融合している。メッシュを使うとスイッチングハブは環状、パラレル接続、両方混合のメッシュだろうと、どんな方法でも接続できる。リンクはすべてアクティブなままで、負荷はリンクアグリゲーションのようにリンク間で分担される。専用のメッシュアルゴリズムは魔法でもかけたようにループを排除し、それでいて見境なくリンクを無効にすることはないし、パケットが際限なく回り続けることがないようにしてくれる。

メッシュは故障時の切り替えも早く、バンドワイズを追加してくれるリンクアグリゲーションと、スパニングツリープロトコルの柔軟性を併せ持っている。そしてリンクアグリゲーション同様、スイッチングハブを配置するときメッシュに参加するポートを手作業で識別しなければならない。

音声インタフェースの有効性

CobraNet はネットワークへの音声インタフェースで高可用性を実現する手段をいくつか提供する。

インタフェースデバイスを対にする

複数の CobraNet デバイスに同じバンドルでの送信を割り当てられる。コンダクタが送信許可を出すのは 1 台のデバイスだけだ。許可を受けたデバイスに異常があれば許可はもう 1 台のデバイスに譲られる。すべてのデバイスで同じ音声情報ソースを送信すれば、この単純な設定でバックアップを作れるのだ。

複数の CobraNet デバイスで同じマルチキャストバンドル受信するよう設定できる。設定されたデバイスはすべて同じ音声を受け取ることになるだろう。また複数の受信機に同じユニキャストバンドルを割り当てることができる。音声を受信するのはそのうち 1 台だけだ。その受信機に異常があれば他のデバイスが受信する。どのスキームでもデバイスの音声出力をすべてアナログ領域で結合することができるため、より丈夫なシグナルを生成することができる。

バディリンク

バディリンクは上記で述べたバックアップペアを改善したものだ。バディーリンクはプライマリデバイスとセカンダリデバイスをクロックで接続する。プライマリが適切に機能しているときはセカンダリの入力にクロックが届いている。このためセカンダリデバイスはネットワークに参加できないのだ。プライマリデバイスに異常が発生するとクロックが届かなくなるため、セカンダリがすぐに取って代わる。

デュアリンク

多くのシステムデザインでは Ethernet スイッチングハブの 1 点が故障するとシステムの本質的な部分に影響する。特別に考えるまでもなく、スイッチングハブが壊れれば接続しているすべてのデバイスに障害が起こる。こうした重大なパーツを 2 つの別個のネットワークに接続すれば危険を緩和できるだろう。このアプローチはふだんデータ通信ネットワークに使われている。サーバに複数の NIC を搭載しておき、ネットワークの異なった部分に接続して故障に強いシステムにするのは当たり前の手法なのだ。

CobraNet インタフェースの最新バージョンCM -1 ではデュアリンクと呼んでおり、2 つの Ethernet 接続をサポートする。プライマリポートが接続できなくなればセカンダリに切り替わるのだ。

ネットワークを混在させる

CobraNet とデータ通信トラフィックを 1 つのスイッチング Ethernet に共存させることができる。しかしデータ通信トラフィックは大きく変化しやすいので数量化しにくい場合がある。データ通信のバンドワイズ要求は、パソコンがアイドリング状態のときはほとんど0なのに対して、大きいファイルを伝送しているときはフルの 100Mbit に到達することがある。一方 CobraNet のトラフィックは音声チャンネルごとにおよそ 1Mbit で一定している。

シンプルな設計でネットワークを共用してもすべてうまく動くだろう。しかしそのネットワークで誰かがブリトニー・スピアーズの海賊版ビデオをサーバーにコピーする日が来るかもしれないし、そんなことになればデータ通信のトラフィックは天井を突き抜ける。ネットワークは部分的にあふれかえることになり、パケットが無差別に失われることもあるだろう。欠落するデータは CobraNet の音声かも知れないし、ブリタニーのへそかもしれない。

いったいどうしたものだろうか。ページングシステムでたまに音声が欠落してもたいしたことはない、という場合もあるだろう。ネットワークに接続したパソコンで使用できるアプリケーションを制限することもできるだろう。インターネットの閲覧とほとんどのシステム制御・監視機能はバンドワイズを限定する。CobraNet のために別のネットワークインフラを導入することになるかもしれない。あるいはこれから紹介する治療法を考慮に入れてもいい。

ブロックしないスイッチングネットワークデザイン

ネットワークは想像しうるトラフィックのパターンに適したふさわしいバンドワイズを確保するよう設計できる。以前はこうした設計にお金がかかったのでできない相談だった。しかしギガビット Ethernet の到来によっては特に小規模から中規模の設備でいっそう実行可能なものになったのだ。

ブロックしないスイッチングネットワークの設計例を図 7.4 と 7.5 に示した。

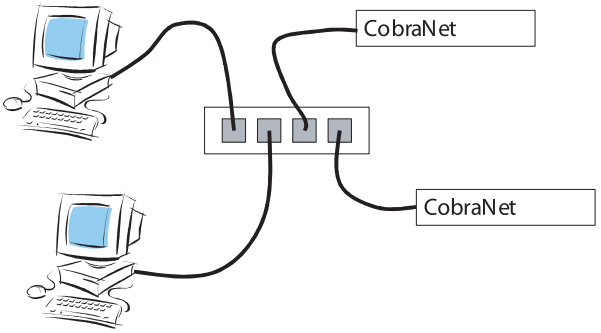


図 7-4

近年のスイッチングハブでは内部のバンドワイズを単純なブロックしないネットワークで保証している

バーチャル・ローカルエリア・ネットワーク

CobraNet と同じネットワークにあるデータ通信アプリケーションの相互作用を制限する手段の 1 つがバーチャル・ローカルエリア・ネットワーク (VLAN) だ。これはスイッチングハブをパテーションにして相互作用しないネットワークドメインに分割することで実現する。注意すべきことは、データ通信が CobraNet の音声に影響を与えないようにすることはできるが、パソコンと CobraNet デバイスの間でも伝送能力がなくなる点だ。これではデータネットワークから CobraNet デバイスを監視したり管理することができない。この問題については後で結論を申し上げよう。

VLAN を使うには VLAN をサポートしたスイッチングハブ (管理機能を持つスイッチングハブはたいていサポートしている) が必要で、それを手作業で設定して特定のポートを特定のバーチャル・ネットワークに割り当てなければならない。

図 7.6 には同じネットワーク上でデータ通信と CobraNet トラフィックを分離するための VLAN を紹介した。

さらにバーチャルコンセプトを一歩進め、VLAN にタグを付けて 1 つのアップリンクに両方の VLAN のデータを多重送信させることができる。これならネットワークの柔軟性を向上して配線の複雑さを減らせるが、共有したリンクでデータと音声ネットワークが相互作用する可能性も生まれる。

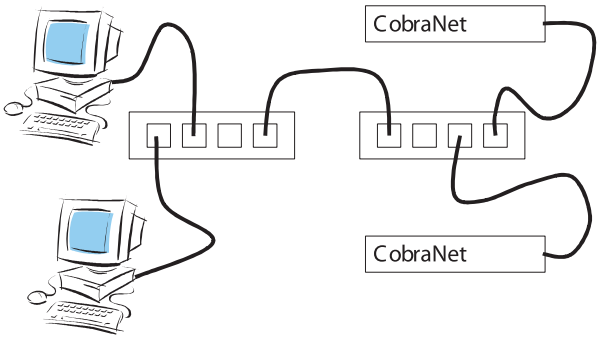


図 7-5

この例ではスイッチングハブ同士のリンクがボトルネックになりやすい。この場合トラフィックのほとんどは PC 同士あるいは CobraNet デバイス同士の間にある。問題のリンクはバンドワイズの低い制御と監視のデータを転送しているだけだ。

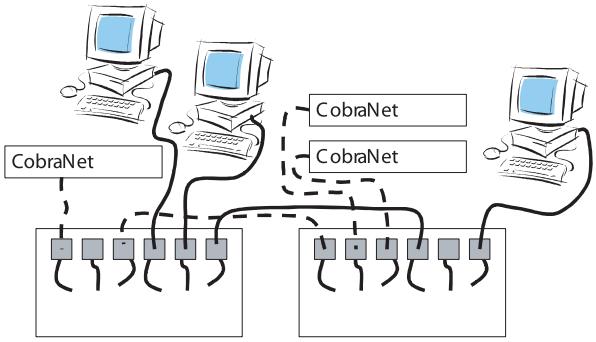


図 7-6

同じネットワークの中で VLAN を使い、CobraNet トラフィックを分離した例。この簡単な例では VLAN 同士がアップリンクされている。

QoS

QoS と CoS は費用効果が高いネットワークデバイスで、広まりつつある洗練された機能だ。QoS はネットワークトラフィックに相対的な優先順位をつけられるようにするものだ。重要なトラフィックを識別するときはネットワークアドレスやポート番号、VLAN に参加しているかどうか、あるいはプロトコルでも指定できる。QoS を導入するときはネットワークを構成するスイッチングハブを注意深く設定しなければならない。

QoS が登場するのはポートやリンクがあふれたときだ。トラフィックが識別され、重要性の低いラフィックを落としてよ

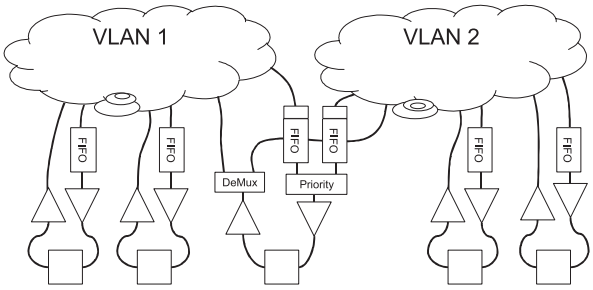


図 7-7

タグ付き VLAN と QoS に対応するスイッチングハブの例。共用している中央のポートを経由したパケットには VLAN メンバーのタグが付けられる。このポートには QoS が設定されている。

り重要なデータを優先する。

QoS が最も一般的に使われているのは、スイッチングハブ同士を接続した負荷が大きくなりやすいアップリンクポートを調整するときだ。この方法を使えば複数の VLAN でトラフィックの不本意な相互作用なくしてアップリンクを共用することができるのだ。

大きな設備

大規模なプロジェクトでは一般的に音声の専門家と共に IT のエキスパートも呼ばれてシステムの設計やコミッションを依頼される。新しいデジタル世界の秩序では、音声と IT の専門家がその施設の現在の、そして未来の必要条件を満たすシステムを構築するために共同して働かなければならない。以降では大型システムのソリューションについて紹介しよう。

コアスイッチを使う

Ethernet ネットワークはスター形状で配線される傾向がある。ネットワークが小さければスターは 1 つで良いだろう。中規模の設備がではいくつかのスターを接続することになる。より大きな設備ではスターでスターを構成するのが最も適切だ。この中心にコアスイッチと呼ばれる大容量のスイッチングハブを置く。コアスイッチはネットワークの中心であり、故障しやすいポジションの1つだ。このためたいていのコアスイッチは小さい冷蔵庫ほどのサイズで、ホットスワップ対応の電源やインタフェースカードのようなバックアップ機能を数多く装備している。図 7.8 のように重要で大きなネットワークの多くがバックアップと対になったコアスイッチを使っている。

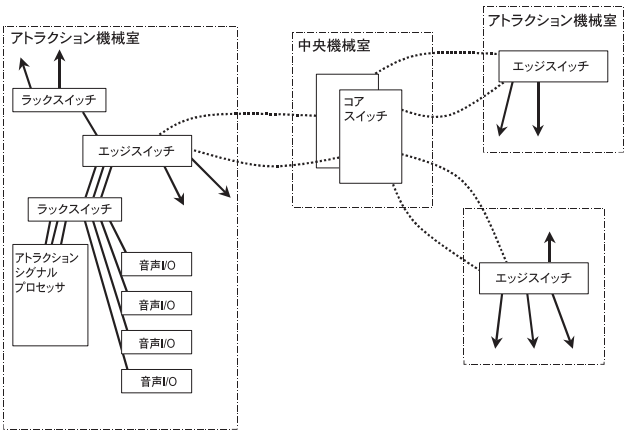


図 7-8　バックアップ用コアスイッチを含むテーマパークの例

音声の VLAN

CobraNet 自体、スケール上の制限がある。最初の (そして唯一の) 制限がマルチキャストバンドルトラフィックに対する限度だ。マルチキャストトラフィックはネットワーク上のすべてのステーションに伝送されるが、このトラフィックはネットワーク全体で受容できるよう制限されているのだ。マルチキャストのトラフィックを管理するときの詳細なガイドラインは「Bundle Assignments in CobraNet Systems」で紹介している。Peak Audio のウェブサイトでダウンロードできるので下記のパスを参照していただきたい。

http://www.peakaudio.com/cobranet/papers/Bundle_Assignments.html.

マルチキャストが限界に達した場合には2つのオプションがある、マルチキャストをユニキャストに変換するか、ネットワークを別個の VLAN に分けることだ。

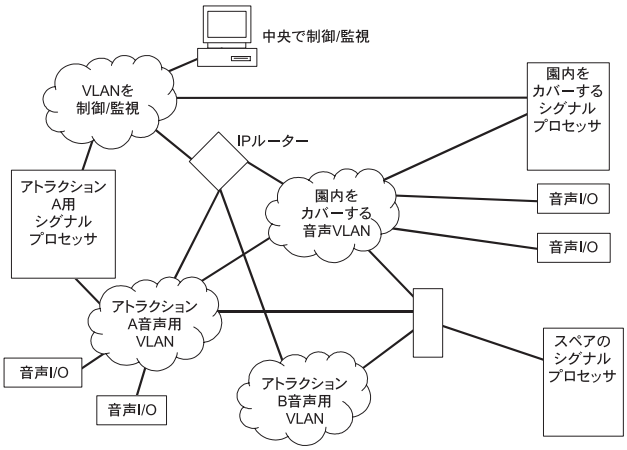


図 7-9

テーマパークでレイヤー 3 ルーティングしている例。菱形のものがレイヤー3ルーティングの要素。場合によってはこの要素は別のハードウェアになっていることがあるが、一般的にはコアスイッチの機能の 1 つでソフトウェアになっている。

大きな設備で音声の VLAN を使用することは、管理の見地からも意味がある。大きなシステムはしばしば小さなサブシステムを相互接続した集合体と見なされる。VLAN はサブシステムの境界線を定義して、サブシステム間に不要な相互作用がないことを保証するのだ。

レイヤー 3 ルーティング

大きなネットワークは一般に VLAN を通して複数のドメインに細分される。このとき別のドメイン同士で通信することは不可能だ。音声トラフィックを尊重してドメイン同士を分離したままにするのは良いことだが、制御と監視のトラフィックがドメイン間を自由に流れるようにした方がもっと望ましい。

レイヤー 3 ルーティングならこれを達成することができる。

レイヤー 3 は OSI ネットワーキングモデルを表したもので、公共のインターネット上で使われるルーティングだ。ネットワークがますます大きくなるにつれて、このような概念の使用がいっそう貴重になる。図 7.9 に大きいテーマパークでのルーティングのユーティリティーを示す。

距離とスイッチホップ

大きなシステムでは、データは目的地まで長いケーブルやファイバー、大量のネットワークデバイスを通過しなければならないことになる。CobraNet はリアルタイムシステムであり、確実に音声が分配されるために必要なネットワーク特性条件を決めている。特性の必要条件は「Protocol Description and Timing Practices」で紹介している。下記ウェブサイトで参照されたい。

http://www.peakaudio.com/cobranet/developer/protocol.html.

これらの必要条件の核は、フォワーディングディレイに関するソフトウェアの要求と、ディレイの変化に関するハードウェアの要求だ。

フォワーディングディレイ

CobraNet は正確に 256 サンプルの期間 (5-1/3msec) ですべての音声分配を保証している。しかしこれはフォワーディングディレイが仕様を満たしているネットワークの場合だ。フォワーディングディレイの仕様を越えたネットワーク上では、受信機が自動的に 64 サンプル分 (1-1/3msec) のレイテンシーをバンドルごとに追加する。フォワーディングディレイの仕様を極端に外れるとレイテンシー追加が保証されない。これはネットワークを通過するときのパスによる変化、あるいはネットワークにおけるコンダクタの位置によって変化する。受信機は SNMP を通して、追加のディレイがどのぐらい受信したバンドルに加えられたか見ることができる。

データが通過するスイッチングハブの数を制限することは主に、フォワーディングディレイを制御するためだ。100Mbit のスイッチングハブはおよそ 150 μ sec のフォワーディングディレイを追加する。同様にリンクスピードを上げればフォワーディングディレイは減少する。100Mbit ファスト Ethernet のフォワーディングディレイに比べ、10 倍速いギガビット Ethernet の場合は 10 分の 1、15 μ sec だ。

ネットワークトポロジーを総点検することはスイッチホップを減らす最も有効な手段だ。スタートポロジーならホップ数を最低できる。

光に普遍の速度があるため、ケーブルもわずかなフォワーディングディレイをもたらす。通常これらのディレイは取るに足りないが、かなり大きなシステムでは重要になることもあるだろう。光ファイバーケーブル 2km 分のフォワーディングディレイはおよそ 20 μ sec だ。80km 引き回せば 800 μ sec になる。静止軌道上の人工衛星にデータをバウンドさせると 750msec にもなるのだ。

遅延の変動

遅延の変動はやっかいな仕様だ。これが仕様を超えているとCobraNet は機能できない。CobraNet ではビートパケットの到着時間にローカルクロックを合わせる方法でサンプルクロックが分配されている。ネットワークで遅延が変動したためにビートパケットの到着時間が予測できないことになれば、そのデバイスはサンプルクロックでネットワークにきちんと同期できないことになる。有効なサンプルクロックがなければ音声の送信と受信は停止するのだ。

遅延の変動はデータがスイッチングハブを通過するときに発生する。スイッチングハブを通過するときにかかる時間は必ずしも一定ではなく、特にスイッチングハブに負荷がかかっていたり、伝送中のパケットが通過を待たされればよけい長くなる。スイッチングハブを通過するときの遅延がフォワーディングディレイで支配されているシステムでは、遅延の変動はフォワーディングディレイに比例する傾向がある。Peak Audio では一般的なルールとして、7 台を超えるスイッチングハブを経由しないよう提案している。このガイドラインは遅延の変動 (必ずしもフォワーディングディレイではない) を仕様の範囲内にとどめようとするためのものだ。スパニングツリープロトコルやメッシュでもネットワーク直径がスイッチングハブ 7 台に制限するよういわれている。

Chapter 8　音声ネットワークのトラブルシューティング

はじめに

音声ネットワークのトラブル解決について理解することは、アナログ音声システムでどうトラブルに対処するかを理解することと同じぐらい重要だ。

物事がすぐに機能しないように思えたら、ここで紹介するアドバイスがいっそう早く、そして効率的に問題の本質に到達する手助けになるかもしれない。

当たり前のことを確認する

問題はとても明白で調べようと思わないような箇所で発生することがある。この種のトラブルで最も多いのが、すべての機器に電源が入っているか？というやつだ。常にすべての機器に電源が接続されていて、電源スイッチが入っていることを確認しよう。

リンクを調べる

たいていのネットワーク機器には、前面や背面にリンクの状態を表示するインジケーターが付いている。リンクはネットワークが正常に動作するために必要だ。リンクがなければ下記の事柄を調べてみよう。

ケーブルはきちんと接続されていてジャックは奥まで差し込まれているだろうか。RJ-45 ジャックをしっかり差し込まないとリンクが確立できないことがある。

ジャックを差し込み直しても機能しない場合は、パス上の他のポイントでケーブルが損傷している可能性もある。ケーブルが正常かどうかを確認する最も簡単なチェック法は疑わしいケーブルを正常なケーブルに交換してみることだ。

スイッチングハブのポートでリンク LED が点灯していない場合は、そのポートに欠陥があることも考えられる。疑わしいポートから正常なポートにケーブルを移動してみよう。

それでも問題が解決しないようならスイッチングハブの設定が間違っているのかもしれない。スパニングツリープロトコル、メッシュ、トランキング、VLAN など進歩的な機能を使っていない場合は、スイッチングハブを工場出荷時のデフォルトにリセットしてみよう。

管理機能を持つスイッチングハブの設定

管理機能のないスイッチングハブを使っている場合はおそらく設定内容を調べる必要はないだろう。しかし管理機能を持つスイッチングハブを使っていて以前はリンクが確立されていたなら、スイッチングハブの設定を再確認してみよう。

CobraNet デバイスはオートネゴシエーションしてそのネットワークがスイッチングとリピーターのどちらであるか認識している。つまり TX ポートはすべてオートネゴシエーションできるよう設定しておかなければならないのだ。オートネゴシエーションが不可能な (スイッチングハブのポートを手作業で設定する) 場合、CobraNet デバイスはリピーターハブに接続していると想定してハーフデュプレックスの接続を確立する。たとえスイッチングハブのポートがハーフデュプレックスに設定されていた場合でも、CobraNetデバイスはリピーターネットワークに接続しているものと考えてコリジョン回避メカニズムを作動させてしまうだろう。このモードで動作するとスイッチングネットワークには対応できても音声が断続的に再生される場合もある。

光ファイバーを使っていてオートネゴシエーションできない場合、すべてのポートは 100Mbps のフルデュプレックに合わせるよう手作業で設定しなければならない。不釣り合いだったり不適当な操作モードにすると特性を損なったりパケットが損失する。

ネットワーク上に環状接続がある場合はスパニングツリープロトコルやメッシュをすべてのスイッチングハブに適用しなければならない、ということもお忘れなく。

LED がエラーを示しているか?

この場合はシステム中のどこかでケーブルが損傷している可能性がある。製造上の欠陥やペアがきちんとツイストされていない、ケーブルタイプの間違いなどが問題を起こすこともある。通常の電話線や CAT3 ケーブルを使うとひどい結果になる。

正しくない種類の RJ-45 コネクターを設置した可能性もある。間違ったコネクターの使用が断続的な再生や高いインピーダンスをもたらす。

音声をチェックしよう

一般に、システムを単純化することを恐れないようにしよう。可能な限り中間のコンポーネントを取り除き、送信機から受信機に直接音声を送る努力をしよう。

信号の有無

音声デバイスに信号が来ているかどうか、利用可能などんな表示器でもチェックしよう。音声は入力に来ているだろうか。来ているとすれば出力に問題があるかもしれない。

来ていなければ当たり前のことを確認しよう。音声ネットワークデバイスの電源は入っているだろうか、音源の電源スイッチは入っていて正常に再生しているだろうか。

音声信号は出力に来ているだろうか。それなら問題はさらにシグナルパスの下流にあるかもしれない。

バンドル番号は正しいだろうか。CobraNet のバンドルアサインが適切であるかどうかを確認しよう。送信側が 301ch で送信しているのにどのデバイスもそのチャネルを「聞いて」いなければ音声は伝達されない。

音質

耳は時折最高のトラブル解決ツールになる。音声信号を聞いてみよう。歪んでいるだろうか。

歪んでいる場合はその種類が重要だ。歪みはすべてのレベルで等しいか、あるいは高いレベルのときだけだろうか。歪みの種類によって原因が違うこともある。

アナログが過負荷になったときのように高いレベルでだけ歪むなら、最高のアナログスキルを駆使して問題を解決しよう。ゲイン構成は正しいだろうか、クリップしているのだろうか、マイクレベルの入力にラインレベルの信号を接続していないだろうか。

どのレベルでも歪んで聞こえるならネットワークがドロップアウトしているかもしれない。ドロップアウトの原因はリンクが負荷であふれかえったせいかもしれないし、破損したり間違ったケーブルが原因になっていることもある。

デジタル音声は「全部か無か」の動作をする傾向がある。通常音声が出て入れば問題がない。しかしアナログ音声のように断続的だったり限界に近い状態はあり得ることだ。こうした状態が音声に違った現象で現われるが、それは音声ネットワークをパケット化する方法による。パケットが損失すれば音声に小さな穴が開くことになるが、この穴がとても短い (1msec 程度) ので欠落というより歪みに聞こえるのだ。高い信号レベルでなくても歪みが聞こえるようなら、おそらく実際にはパケット損失だと考えて良い。

最終的に、すべてのチャンネルが受信されていることを保証するために調べよう。

バンドルナンバーが正確に割り当てられていることを、そしてもう一度、当たり前のことをチェックしてみよう。